Money, Cryptocurrency, and Monetary Policy

Kee-Youn Kang* Seungduck Lee**

December 19, 2018

Abstract

Can a cryptocurrency, Bitcoin, compete with central bank-issued money as a medium of exchange? We develop a search theoretic model where both money and Bitcoin can be used as a means of payment in transactions, and currency choices are endogenously determined. We analytically study the necessary condition for the coexistence of money and Bitcoin in equilibrium. We also calibrate the model to quantitatively study the effects of monetary policy and an increase in Bitcoin transaction fees on the economic activities and welfare. Our analysis shows that Bitcoin can meaningfully compete with money only when the inflation rate is sufficiently high, and also that the economic welfare in an economy with both money and Bitcoin is lower than that in a money-only economy due to the current inefficient mining process of Bitcoins. The welfare gap between the two economies expands as inflation rate increases. Furthermore, transaction fees for Bitcoins increases welfare in an economy where money and Bitcoin coexist.

JEL Classification: E31, E50, E52, G12

Keywords: Money, Cryptocurrency, Bitcoin, Digital currency, Blockchain, Monetary Policy, Medium of Exchange

* Yonsei University, keeyoun@yonsei.ac.kr, ** Sungkyunkwan University, seung.lee@skku.edu.

We are grateful to Kyu-Hwan Cho, and Yong-Gu Kim for their useful comments and suggestions and Jong-Ik Park for the calibration data. We would also like to thank participants at the talks at Sungkyunkwan University, Yonsei University, the Bank of Korea, Korea University, and the Korea International Economic Association. This paper was supported by the Bank of Korea's Research Fund in 2018. The views expressed herein are those of the authors and do not necessarily reflect the official views of the Bank of Korea. All errors are ours.

1 Introduction

Since Bitcoin was introduced in 2009, more than 1,600 cryptocurrencies have been created and traded online as of September 21, 2018. Most of them have been designed for "a purely peer-to-peer version of electronic cash" as presented in Nakamoto (2009), even though they have not been used much as a medium of exchange (henceforth, MOE) in commodity transactions so far. Among others, Bitcoin has several noteworthy records. Bitcoin, followed by Etherium and Ripple, is the top-ranked cryptocurrency in terms of market capitalization and daily trade volume, amounting to $112 billion and $ 5 billion as of September 21, 2018, respectively.[1] Moreover, the dollar price of one Bitcoin (BTC) recorded an all-time high of $19,783.06 on December 17, 2017.[2] These records of Bitcoin have drawn a lot of attention from not only the public, but also policy makers. However, our understanding of cryptocurrencies as an MOE is limited despite of its relevance to economic activities.

Recently, international organizations such as Bank for International Settlement (BIS) as well as central banks, such as Bank of England and Bank of Canada, have started intensive research on cryptocurrencies.[3] However, this work is in its early stages. Furthermore, economics literature has so far provided little insight on it;

[1] Source: https://www.coinlore.com. The market capitalization of Morgan Stanley was 100.07 billion dollars as of January 2018, which is the fifth largest bank in the U.S. in terms of market capitalization.

[2] Source: http://fortune.com/2017/12/17/bitcoin-record-high-short-of-20000/

[3] The Bank of International Settlements evaluated and discussed cryptocurrencies and their technology in existence in a chapter of its annual report, released on June 17, 2018. The Bank of England released a report, titled 'One Bank Research Agenda' in February 2015 where research on digital currency or cryptocurrency is included as one of the five key themes. Similarly, the Bank of Canada has also begun research on it as a theme in 'The Bank Medium-term Research Plan, 2016-2018'. The Bank of Korea launched a task force for research on digital currencies in 2017.

there are still many questions to be answered academically. Among others, we need to answer the following questions: can a cryptocurrency coexist or compete with the central bank-issued money? If so, how do monetary and fiscal policies affect their coexistence? Further, how do these policies and Bitcoin transaction fees affect the cryptocurrency-related activities such as the trade volume of cryptocurrency, and economic welfare? Does the coexistence of money and a cryptocurrency improve economic welfare?

We address the above questions by developing a monetary search model in which the central bank-issued fiat money (henceforth, *money* in short) and a cryptocurrency are used as an MOE. In particular, we incorporate technical features of Bitcoin, a representative blockchain-based cryptocurrency, into the *Lagos and Wright (2005)* framework. This is not only because Bitcoin is the first cryptocurrency that was built on the blockchain technology, but also because alternative cryptocurrencies, such as Bitcoin Cash, share most of the technical elements of Bitcoin. Thus, it is true in reality that the term 'Bitcoin' is widely used to represent a cryptocurrency and they are oftentimes used interchangeably.

Both money and Bitcoin are fiat: they have no intrinsic value in the model as in reality. Both can be used as an MOE in transactions, and agents are allowed to choose either money, Bitcoin, or both to transact in exchange for goods. However, there are differences between money and Bitcoin in terms of their usefulness in facilitating transactions as follows. The government imposes sales taxes on transactions where money is used as an MOE. On the other hand, there is no sales tax on transactions where Bitcoin is used as an MOE as in reality. Instead, buyers pay transaction fees to buy goods with Bitcoin to a third party, so called *miners* in the

Bitcoin system, who validate the ownership of Bitcoin spent and record its changes in a digital (distributed) ledger. Since Bitcoin is a digital currency, the existence of miners for validation and record-keeping is essential so that Bitcoin can be a means of payment in transactions. Importantly, unlike money, a positive mass of time is required for miners to finish validating and recording transactions, so called *mining* in the Bitcoin system. The time required for the mining work can make sellers reluctant to deliver goods on the spot, because they cannot be sure whether the ownership is completely transferred to them until mining finishes. This implies that buyers can be required to wait a certain period of time before receiving goods. The delayed delivery of goods limits the ability of Bitcoin to facilitate transactions as an MOE. Finally, mining requires miners' efforts, which causes welfare loss because the efforts do not produce any consumable goods. Meanwhile, the government has to pay for the money operation cost to facilitate the role of money as an MOE, that is, printing new currency, transportation, and destruction of mutilated currency. More details about the features of Bitcoin that we incorporate into the model are described in Section 1.2.

Although it is always possible that only one type of currency is used as an MOE in equilibrium, we focus on the equilibrium in which both money and Bitcoin coexist as an MOE. In order for both to coexist in equilibrium, agents must perceive money and Bitcoin as an MOE indifferently. In particular, the model suggests that if the money growth rate is lower than a certain threshold level, then money and Bitcoin cannot coexist, because the former is strictly more useful than the latter as an MOE. However, this does not mean that an equilibrium where Bitcoin is the only MOE cannot exist. Depending on the agents' expectation in our model, it is

always possible that only Bitcoin is used as an MOE and money is not valued in equilibrium independent of the money growth rate, because both currencies are fiat.

To obtain more implications, we calibrate the model to the U.S. economy, and conduct a quantitative analysis. A key insight of our analysis is that an economy with only money as an MOE (henceforth, *money-only economy*) accomplishes higher levels of economic welfare than an economy where both money and Bitcoin work as an MOE (henceforth *coexistence economy*) does. As explained above, when buyers purchase goods in exchange of Bitcoin, a delay in the delivery of goods may occur because of the mining process itself. The delayed consumption generates utility loss in addition to the welfare loss caused by the costly mining work. This implies that Bitcoin is not as efficient as money as an MOE. Our quantitative analysis shows significant losses under the current Bitcoin system. In the coexistence economy, money can be substituted with Bitcoin, which is less efficient as an MOE, when inflation rate, that is, the cost of holding money, is positive. Consequently, the money-only economy achieves higher economic welfare than the coexistence economy.

As the inflation rate increases, the aggregate quantity of trade and welfare fall in the both money-only and coexistence economies, because of the increased money holding cost. Interestingly, the welfare gap between the two economies widens. Agents in the coexistence economy can substitute away money with Bitcoin. As the inflation rate increases, this substitution decreases transactions with money, but increases transactions with Bitcoin. The aggregate quantity of traded goods shows a lower decrease in the coexistence economy than in the money only economy. However, an increase in the aggregate Bitcoin trade volume leads to an increase in the

average waiting time until a new Bitcoin transaction is validated and recorded in the Bitcoin system. The delivery of goods purchased with Bitcoin can be delayed for a longer time on average, and thus the *effective* consumption of buyers, which takes account of a consumption delay, lowers compared with the effective consumption in the money-only economy. Thus, the welfare falls further down in the coexistence economy than in the money-only economy in response to an increase in the money growth rate, and the welfare gap between two types of economies widens.

Finally, we analyze the effects of the Bitcoin transaction fees on economic activities and welfare. A key result is that, as the Bitcoin transaction fees increase, welfare increases in the coexistence economy, while it decreases in an economy in which Bitcoin is used as the only MOE (henceforth, *Bitcoin-only economy*). The transaction fees play a role as the Bitcoin holding cost, as inflation does in a standard money search model. As the transaction fees increase, the Bitcoin trade volume decreases and welfare declines in a Bitcoin-only economy. This result is consistent with one of the main findings in Chiu and Koeppl (2017), who study the optimal design of the Bitcoin system. Interestingly, however, welfare increases in response to an increase in the transaction fee in the coexistence economy. When both money and Bitcoin are used as an MOE, agents can substitute Bitcoin with money, which is a more efficient MOE, as the transaction fees increase. Hence, the aggregate trade volume less decreases compared with in the Bitcoin-only economy. Furthermore, the decrease in the Bitcoin trade volume leads to a decline in the average waiting time for confirming Bitcoin transactions, which makes Bitcoin a more efficient MOE. As a result, economic welfare increases as the transaction fees increase in the coexistence economy.

1.1 Related Literature

The economics literature on cryptocurrencies based on the blockchain technology has been limited so far, in spite of the recent rapid growth. Our study can be considered a part of the literature on coexistence and substitutability of the central bank-issued money (or so-called "outside" money) and privately issued monies (or "inside" money), such as Kocherlakota (1998), Kocherlakota and Wallace (1998), and Cavalcanti and Wallace (1999). Fernández-Villaverde and Sanches (2016), whose work is close to our study, build a theoretical framework with digital currencies in order to study currency competition between the central bank-issued money and a private digital currency, and then the effect of monetary policy on the competition. They conclude that a privately-issued digital currency which is not backed by productive capitals might be driven out of the economy. However, cryptocurrencies were not seriously considered as one of privately issued monies in these studies. That is, the main features of the blockchain-based cyrptocurrenies such as a mining process of new blocks were not explicitly incorporated in the framework with the central bank-issued money. To the best of our knowledge, our work is the first attempt to study how the central bank-issued money and a cryptocurrency coexist and compete within a theoretical framework including the key features of blockchain-based cryptocurrencies.

Some recent literature has addressed questions which focus on the Bitcoin system, a representative cryptocurrency system itself. For example, Chiu and Koeppl (2017) study the optimal structure of the Bitcoin system. They demonstrate that the efficiency of the Bitcoin system can be improved by changing its reward mechanism for mining. Specifically, they show that reducing transaction fees and controlling

the new coin creation rate can decrease the welfare loss from 1.41% to 0.08%. Cong et al. (2018) examine the dynamic pricing of cryptocurrencies, or crypto-tokens, on an online platform. They focus on a user-based externality, called a *network effect* on a blockchain platform where cryptocurrencies are created and used for transactions. In their analysis, the growth effect of the tokens, caused by the externality, can increase welfare and reduce the volatility of user adoption, and thus price variation. However, both studies investigate the economy only with a cryptocurrency, especially Bitcoin. Similarly, Gandal and Halaburda (2014) study network effects on competition among crytopcurrencies and their relative valuation. Chiu and Wong (2015) take a mechanism design approach to discuss how *e*-money helps in implementing constrained efficient allocations. *E*-money is also a digital currency, but its technical background differs from the blockchain-based cryptocurrencies. None of these studies examines how a cryptocurrency competes with the central bank-issued money, and thus how monetary policy affects cryptocurrency-related activities and economic welfare in an economy with both money and a cryptocurrency as in our work.

Besides, there are some studies in the international macroeconomics and finance literature, such as Routledge and Zetlin-Jones (2018), who show that blockchain distributed ledger technologies, which support most of cryptocurrencies, can be used to establish currency stability against another currency by removing self-fulfilling speculative attacks on a currency in a model with bank runs of Diamond and Dybvig (1983). In addition, Gandal et al. (2017) and Glaser et al. (2014) focus on cyptocurrency valuation and its volatility as a store of value, not an MOE.

1.2 A brief introduction of cryptocurrencies

In this subsection, we describe the main features of blockchain-based cryptocurrencies, in particular, Bitcoin, in order to understand how we incorporate those features in the model. Among several technological features, we focus on the monetary characteristics of cryptocurrencies as an MOE rather than the blockchain technology itself.

Technological progress allowed financial institutions to digitalize the existing physical currencies which are deposited into financial accounts. Digitalized, or digital, currencies necessarily require trustworthy record-keepers and electronic ledgers, where the current status or changes of its ownership are electronically recorded by a series of numbers—a combination of either 0 or 1. The main concern with this feature is that the records can be easily duplicated into other digital memory devices. It can cause a double spending problem; for instance, the same digital token can be spent more than once. The double spending risk is inherent in all the digital currencies in existence. The digital currencies in existence before the recent emergence of cryptocurrencies have been eliminating the double spending risk mainly by authorizing only few of legally qualified financial institutions to record currencies' ownership and keep it on their own digital ledgers.

Cryptocurrencies are also a kind of digital currency which exist only in the form of electronic records on digital ledgers, and are thus exposed to a double spending risk. Unlike the existing digital currencies, cryptocurrencies remove this risk by using the blockchain technology for recording and record-keeping. The blockchain is a digital ledger in which anyone can record and keep the complete transaction history only if he/she is willing to do it. As a representative example, the Bitcoin

system authorizes so-called *miners* to validate and record Bitcoin transactions or changes in its ownership through a *node* on the blockchain. Being a miner implies being connected through a node to the Bitcoin network. A node is a program which validates new transaction records, broadcasts blocks with the records to other nodes, and keeps the chain of blocks.[4] Anyone can be a miner only if he/she installs Bitcoin-mining computer programs online, which enables the miner to validate, record, and maintain changes in Bitcoin ownership through a node and to be connected to the Bitcoin network.

Specifically, miners compete with one another to be the only one who records transactions on the blockchain and earns rewards for it. To win the competition, a miner makes or *mines* a new block with collected pending Bitcoin transaction data by finding out a cryptographic nonce to compute a specific hash value through the hash function dSHA256, and spreads the block to other nodes on network.[5] If more than a half of the total nodes accept and miners on the nodes use the spread block for the next block creation by attaching it to the chain of existing blocks, then the miner becomes the only winner and receives the rewards.[6] Since the number of nodes who accept the newly created block must be more than 50% of the total number of miners for winning the competition, the blockchain is oftentimes called an "agreed-upon shared distributed database." The current Bitcoin system is programmed to be automatically adjusted for the system stability, such that it takes around 10 minutes,

[4] As of September 21, 2018, 9,575 nodes have been running on the Bitcoin network. Since a node can be shared by several miners, the number of minners in the network is even greater than that of nodes. Source: https://coin.dance/nodes/all

[5] See Berentsen and Schar (2018) for technical details on the block creation process.

[6] We can think of a block as a page in a traditional paper ledger on which transaction records are written and the blockchain as the whole paper ledger. It is natural that additional new transactions cannot be recorded on the ledger without the previously recorded page. In reality, miners are supposed to first attach the most updated block before mining a new block.

on average, to mine a new block, even with advances in the computing technology to calculate nonces and hash values. Lastly, a block size limit of 1 MB (megabyte) per block exists. This implies that a block can contain around 2,000 transactions at most if the size of each transaction record is, on average, 500 bytes. Hence, it can take more time for an individual transaction record to be included in a new block when a large number of transactions occur within a period or the number increases.

Among several consensus protocols, the Bitcoin system adopts proof of work (PoW) as a consensus mechanism algorithm, which is the original one used in the first blockchain network.[7] Miners are supposed to compute nonces to yield specific hash values in order to "mine" a new block. The nonces can be found only through a trial-and-error procedure; hence, this process is called "PoW". PoW requires more than a certain amount of electronic energy and computational usage. Once a miner finds a nonce to a specific hash value, the miner broadcasts the mined block to the network as quickly as possible for verification and consensus. The higher computing power (and thus higher investment cost for the computing power) increases the probability that a miner computes a nonce faster than other miners, and thus wins the competition, that is, adds his/her new block to the blockchain, and obtains the corresponding rewards.

If a miner succeeds in mining, the miner earns two types of rewards: a newly created Bitcoin and transaction fees. The current number of new Bitcoins awarded to a winner is 12.5 Bitcoins. This reward is halved every 210,000 blocks, and Bitcoin creation is scheduled so that the total number of Bitcoin converges to 21,000,000

[7] For example, we can think about Proof of Stake, Proof of Capacity, and so forth as alternative consensus mechanisms that can be used for cryptocurrencies. See Ouattara et al. (2018) for technical details on those mechanisms.

units. In addition, transaction fees are paid for the mining process. The transaction fees incentivize miners to include relevant transactions in new blocks which they create. The current transaction fees remain low, namely, less than 0.001 Bitcoins per transaction, except for some extreme cases. Lastly, Bitcoin awarded as a reward for mining may not be spent for at least the next 100 blocks.[8]

Our remaining paper is organized as follows. In Section 2, we describe the physical properties of the coexistence economy, where the features of the blockchain-based Bitcoin system explained above are explicitly incorporated. In Section 3, we solve economic agents' problems, and in Section 4, we characterize equilibrium. In Section 5, we calibrate the model and conduct quantitative analysis. We conclude in Section 6.

2 Environment

The basic framework of the model is based on Lagos and Wright (2005) with heterogeneous agents similar to Lagos and Rocheteau (2008) and Rocheteau and Wright (2005). Time, $t = 0, 1, ...,$ is discrete and continues forever. Each period is divided into two subperiods when different economic activities occur. A goods market (henceforth, *GM*) opens in the first subperiod and a currency market (henceforth, *CM*) follows in the second subperiod. There is a discount factor, $\beta \in (0, 1)$ between periods. There are three types of agents: buyers, sellers, and miners. There is a continuum of buyers and sellers, each with a unit mass. The mass of miners is

[8]Since mining one block takes currently 10 minutes, on average, successful miners are allowed to spend the rewards in around 16.7 hours. This prevents miners from spending the rewards from a block that may be determined later to be destroyed after a block chain forks.

η, which is endogenously determined in equilibrium. Each agent has the following quasi-linear functional form of preferences in period t:

$$\text{Buyers: } U(q_t, X_t, H_t) = u(q_t) + X_t - H_t$$
$$\text{Sellers: } U(h_t, X_t, H_t) = -c(h_t) + X_t - H_t$$
$$\text{Miners: } U(e_t, X_t, H_t) = -v(e_t) + X_t - H_t.$$

Here, q_t is consumption in the GM; X_t and H_t are consumption and labor supply, respectively, in the CM; h_t is labor supply to produce goods in the GM; and e_t is the effort (or expenses) for mining in the Bitcoin system. $u(\cdot)$ is twice continuously differentiable with the properties of $u' > 0$, $u'' < 0$, $u(0) = 0$, $\lim_{q\to 0} u'(q) = \infty$, and $\lim_{q\to\infty} u'(q) = 0$. Moreover, $c(\cdot)$ and $v(\cdot)$ are twice continuously differentiable, strictly increasing, and strictly convex with $c(0) = 0$ and $v(0) = 0$.

In the first subperiod, the GM opens. Buyers and sellers trade GM goods in a Walrasian market. Buyers want to consume, but cannot produce, while sellers can produce, but do not wish to consume. This generates a double coincidence problem. However, all agents are anonymous—they are unaware of each other's transaction history. Furthermore, they have limited commitment—they are unable to use credit arrangement. An MOE is necessary for transactions between buyers and sellers in the GM. There are two types of currencies that can be used as an MOE: fiat money and Bitcoin. Both are perfectly divisible and storable. Money (M) and Bitcoin (B) grow at the gross rate of γ and γ_b, respectively: $M_{t+1} = \gamma M_t$ and $B_{t+1} = \gamma_b B_t$. We assume that $\gamma > \beta$ and $\gamma_b > 1$.[9] Lastly, miners expend efforts e to validate

[9] In reality, the growth rate of the Bitcoin supply is technically programmed to be positive and to decrease in its supply level. In other words, it positively converges to zero, that is, $\gamma_b \geq 1$.

and record transactions where Bitcoin is used as an MOE. Miners' efforts do not produce any goods.

In the second subperiod, the CM opens. Each agent can produce one unit of the perishable consumption goods or CM goods, for each unit of labor supply. All types of agents trade *numeraire* CM goods and currencies—money and Bitcoin—in a centralized Walrasian market. Any amount of money and Bitcoin can be purchased at prices of ϕ_t and ψ_t, respectively, in terms of numeraire goods in the CM in period t. Money supply is controlled by the government, which is a consolidated authority. New money is injected (withdrawn) into sellers in the CM through lump-sum transfers (taxes) as standard money search models.[10] On the other hand, there is no authority to control Bitcoin supply. The growth rate, γ_b, is determined by the amount of Bitcoin that is newly created and awarded to miners as described below.

Mining work and reward scheme Bitcoin is a digital currency, and thus all Bitcoin transactions are validated and recorded in a decentralized ledger, called the blockchain. A block contains a set of information about all Bitcoin transactions that were conducted between Bitcoin users in a given period, and the blockchain is a sequence of blocks that contains all Bitcoin transaction history.

The issue is, then, who has the right to update Bitcoin transaction information into the existing blockchain, preventing the double spending risk which is inherent in all the cryptocurrencies. First, we assume that any Bitcoin transaction in the CM are automatically recorded to the existing blockchain due to public monitoring. However, we assume that any Bitcoin transactions in the GM must be verified and

[10] In a standard money search model based on Lagos and Wright (2005), the government changes the money supply with a lump-sum transfer to buyers, instead of sellers. However, the identity of who receives the transfer does not affect the main results.

recorded by minors. In the mining process, miners create a new block by expending their own efforts, e, in the GM. The created block contains the information about new Bitcoin transactions in the GM, and is added to the existing blockchain with all the Bitcoin transaction history. We also assume that miners are required to pay a fixed entry cost, $k > 0$, in the CM, in order to join the Bitcoin network and to mine in the next GM. For example, a miner has to pay a cost for being equipped with a computer.

A miner who succeeds in adding his/her new block to the blockchain is compensated with Bitcoin. There are two types of sources for compensation: transaction fees and newly created Bitcoin. First, buyers pay transaction fees to miners in order to purchase goods with Bitcoin in the GM. We assume that the transaction fees are proportional to the total amount of a Bitcoin transaction and fixed at a certain rate of $f > 0$.[11] Second, the miner also receives newly created (or supplied) Bitcoin, R_t, as a reward for his/her successful mining work. The quantity of the new Bitcoin, R_t, determines the growth rate, γ_b: $B_t = \gamma_b B_{t-1} = B_{t-1} + R_t$ (or $R_t = (\gamma_b - 1)B_{t-1}$). Since the reward cannot be negative, we assume that $\gamma_b > 1$ as shown above.

An important feature of the Bitcoin system is that only one miner is allowed to add his/her new block to the existing blockchain, even though any miners can create new blocks. Miners compete with each other to add new blocks to the blockchain, and only one miner receives rewards for his/her mining work. This is called the *Proof of Work* protocol for mining. The probability of winning the competition increases with his/her effort relative to other miners' efforts. For example, a miner

[11] In reality, buyers can determine the transaction fees so that their transactions can be confirmed in the blockchain network as soon as possible. However, we assume that f is fixed because its level has remained stable at a low level since it was invented in 2009. More details are presented in the section on calibration later.

can increase the pace of mining by investing in greater computing power. This increases the probability that the miner can compute a specific nonce faster to create a new block, allowing other miners to accept the miner's new block first.

Confirmation lag of Bitcoin transaction In reality, the Bitcoin transactions are not secured 100% against the double spending risk until a transaction record is a certain number of blocks deep. Thus, sellers may not be sure that a Bitcoin paid in transactions completely belongs to them even if buyers broadcast an electronic message that they have handed over their Bitcoin to the counterpart sellers in the Bitcoin network. In the current Bitcoin system, a transaction record tends to be considered as *confirmed* among Bitcoin users only after the transaction record is at least six blocks deep—if a block that contains a certain transaction record is followed by more than five blocks in the blockchain, then the transaction record is almost 99.9% secured against the double spending risk. Because of the double spending risk, sellers tend to be reluctant to hand over goods to buyers on the spot, even if they electronically receive a message that the buyers paid in Bitcoin for the goods. The sellers are willing to deliver goods only after the Bitcoin transaction is confirmed on the blockchain.

To summarize, when a buyer purchases goods with Bitcoin, a confirmation lag exists; hence, he/she may have to wait for a certain time before receiving goods.[12] We reflect this feature into the model by introducing a discount factor, $\delta \in [0,1]$, to the consumption of goods purchased with Bitcoin, which is similar to Chiu and Koeppl (2017). However, the way of introducing the discount factor is different

[12]Under the current Bitcoin system, it takes 60 minutes on average for a transaction to be confirmed, that is, the transaction record is at least six blocks deep.

from Chiu and Koeppl (2017) in the following sense. There are two types of MOE in our model, and the discount factor, δ, should not affect the consumption of goods purchased with money because buyers receive goods instantly if they pay money. If we introduce δ in front of the utility function, that is, $\delta u(q)$, as in Chiu and Koeppl (2017), it affects the effective consumption of goods purchased with money as well. To avoid this problem, we introduce the discount factor δ inside the utility function $u(q)$, similar to iceberg transportation cost models. The buyer's effective consumption of GM goods in period t is given as

$$q_t^b = q_{m,t}^b + \delta q_{b,t}^b.$$

Under the current Bitcoin system, the time of the confirmation lags depends on two important factors: the aggregate mining effort (ME) and the aggregate quantity of Bitcoin transactions, q_b. Hence, we let the discount factor be a function of ME and q_b, as $\delta(ME, q_b)$, as described below.

First, the mining work is necessary for the confirmation of a Bitcoin transaction. The mining and confirmation processes increase in pace as the aggregate mining effort, ME, increases. For example, if there is no mining work, then a Bitcoin transaction will never be confirmed, and sellers would not deliver goods for perpetuity. Hence, δ would be zero in this extreme case. Following this logic, we assume that the discount factor, δ, is an increasing function of ME and $\delta(0, \cdot) = 0$.[13]

Second, we assume that the discount factor δ decreases in the aggregate trade

[13] Although aggregate mining effort affects the confirmation time in principle, the current Bitcoin system is programmed to be automatically adjusted such that it takes 10 minutes to mine a new block on average. Hence, the aggregate mining effort, ME, does not critically affect the discount factor, and we will use this property to calibrate the model in section 5.

volume, q_b. A new block can contain only a certain number of transaction records due to its size limit of 1 MB. As the Bitcoin transaction volume rises in a given period, more blocks need to be created and be added to the existing blockchain in order. This means that a particular Bitcoin transaction may be contained into the later block of the blockchain. Hence, it can take more time until the transaction is finally confirmed. Thus, we assume that the discount factor, δ, decreases with respect to the aggregate Bitcoin transaction volume as $\frac{\partial \delta(ME,q_b)}{\partial q_b} < 0$ and $\lim_{q_b \to \infty} \delta(ME, q_b) = 0$.

Government expenditure and taxes In typical monetary theories, such as Lagos and Wright (2005), government expenditure is not considered explicitly, and lump sum taxes (or transfers) change passively to changes in money growth rate. However, government expenditure is an important part in the real world, and many quantitative macro models, such as **??**, include government expenditure in their models. We explicitly allow for government expenditure as standard quantitative macro models, but in a stylized way, in order to study a model economy in which money and Bitcoin coexist.

More precisely, government spending in the model comprises government consumption, g_t ,and the cost for the fiat money operations, g_t^m. Government consumption, g_t, includes any expenditure, such as military expenditure and government spending on welfare. We treat it as exogenously given. The cost for the fiat money operations includes printing new currency, transportation, destruction of mutilated currency, verification and removing counterfeit money, and packaging of currency. Although a variety of factors, such as money holding habits of consumers, the denomination system of a country and transaction velocity for each denomination,

affect the money operation cost in reality, we adopt a simple method. We assume that the cost for the fiat money operations is proportional to the real value of money transaction in GM, as $g_t^m = \theta \phi_t \tilde{p}_{m,t} q_{m,t}$, where θ is a parameter that affects the aggregate money operation cost.

We also specify sources of government revenue more explicitly than the previous money search theory. In particular, we include a sales tax as a source of government revenue, which is imposed only on transactions where money is used as an MOE at a rate of τ_m. However, there is no sales tax on Bitcoin transactions. Although other taxes, such as income taxes and capital taxes, are important sources of government revenue and affect agents' economic decisions, we abstract them, such that these taxes are included in lump-sum taxes. We assume that sellers pay the sales tax, but the identity of the sales tax payer does not affect the main results.

Combined together, the government budget constraint is given by

$$\tau_m \phi_t \tilde{p}_{m,t} q_{m,t} + \tau_t + (\gamma - 1)\phi_t M_{t-1} = g_t + \theta \phi_t \tilde{p}_{m,t} q_{m,t} \tag{1}$$

Here, $(\gamma - 1)\phi_t M_{t-1}$ is seigniorage of new money supply given money growth rate γ. τ_t is a lump-sum tax (or transfer if negative) that is determined endogenously given other parameters such as τ_m, g_t, and θ in equilibrium.

3 Economic Agents' Problem

Miners' problem Miners, whose mass, η, is determined endogenously, compete for verifying Bitcoin transactions in the GM, by putting their own efforts, e, in the GM. The probability that a miner i will win the mining competition depends on his

own effort, e_i, and the aggregate efforts of all active miners that are expressed as $ME_t = \int_{j=0}^{j=\eta} e_{j,t} dj$. Each miner takes ME_t as given, and the probability of wining of the miner i is given by $\frac{e_{i,t}}{ME_t}$. The rewards of winning the competition in period t comprise the transaction fees, F_t, and newly created Bitcoins, R_t, and both depend on the the total amount traded and the aggregate quantity of Bitcoin transactions, respectively. That is, $F_t = f\tilde{p}_{b,t}q_{b,t}$ where $\tilde{p}_{b,t}$ is the unit price in Bitcoin and $R_t = r_t q_{b,t}$. If there is no transaction with Bitcoin in a given period, that is, $q_{b,t} = 0$, then there is nothing to verify and hence $F_t = R_t = 0$. The Bitcoin transaction fees are proportional to the total amount traded at the rate of f, but the proportion of newly created Bitcoin to the aggregate quantity of Bitcoin transactions, r_t, is determined by the growth rate of Bitcoin γ_b. More precisely, when $q_{b,t} > 0$, $R_t = r_t q_{b,t} = (\gamma_b - 1)B_{t-1}$. Since we focus on equilibria where both money and Bitcoin are traded, we assume that $q_{b,t} > 0$ and use the equation, $R_t = (\gamma_b - 1)B_{t-1}$, in the following analysis. Finally, a miner has to pay a fixed cost of k in the current CM in order to join the Bitcoin system for mining work in the GM in the next period. Hence, the miner's problem is given as follows in period t.

$$Max\left\{0, \underset{e_{i,t+1}\geq 0}{Max}\left\{\beta\left[\left(\psi_{t+1}(\gamma_b - 1)B_t + fp_{b,t+1}q_{b,t+1}\right)\frac{e_{i,t+1}}{ME_{t+1}} - \upsilon(e_{i,t+1})\right] - k\right\}\right\},$$

where ψ_{t+1} is the real price of Bitcoin in terms of CM goods in period $t+1$ and $p_{b,t+1} = \psi_{b,t+1}\tilde{p}_{b,t+1}$. We discount the expected return on mining work because the rewards are awarded in the next CM, and a miner decides whether or not to pay the entry cost k to join the Bitcoin system in the current period.

In equilibrium, a miner optimally chooses the effort level e given aggregate

miners' efforts ME_{t+1} and must earn zero profit in expectation given the free entry condition. Thus, we obtain

$$\frac{\psi_{t+1}(\gamma_b - 1)B_t + f p_{b,t+1} q_{b,t+1}}{ME_{t+1}} = \upsilon'(e_{i,t+1}) \tag{2}$$

$$\beta \left\{ \frac{\left[\psi_{t+1}(\gamma_b - 1)B_t + f p_{b,t+1} q_{b,t+1}\right] e_{i,t+1}}{ME_{t+1}} - \upsilon(e_{i,t+1}) \right\} = k, \tag{3}$$

as the first order condition and the free entry condition, respectively. The first order condition (2) has a standard interpretation. At optimum, the marginal expected return from increasing the mining effort on the left-hand side must be equal to its marginal cost of this increase in the mining effort on the right-hand side. If a miner increases one additional unit of his/her mining effort, it increases the probability of winning the mining competition, and thus its marginal expected return as on the left-hand side. Moreover, the free entry condition (3) implies that, since anyone can be a miner, the net benefit from mining becomes zero in equilibrium. Since all miners are homogeneous miners, we obtain $e_{i,t+1} = e_{t+1}$ from (2), and thus, $ME_{t+1} = e_{t+1}\eta_{t+1}$.

Buyer's problem Because of quasi linear preferences, it must be $\frac{\phi_t}{\phi_{t+1}} > \beta$ and $\frac{\psi_t}{\psi_{t+1}} > \beta$ in any equilibrium; otherwise an equilibrium does not exist. Then, given $\frac{\phi_t}{\phi_{t+1}} > \beta$ and $\frac{\psi_t}{\psi_{t+1}} > \beta$, a buyer would not bring more than the amount of money or Bitcoin needed to purchase the quantity of GM goods that he/she wants to consume.

Thus, a buyer solves the following problem in the CM of period t

$$\underset{q^b_{m,t+1},q^b_{b,t+1}}{Max} \left\{ \begin{array}{c} -\frac{\phi_t}{\phi_{t+1}} p_{m,t+1} q^b_{m,t+1} - \frac{\psi_t}{\psi_{t+1}} p_{b,t+1}(1+f) q^b_{b,t+1} \\ +\beta u\left(q^b_{m,t+1} + \delta(ME_{t+1}, q_{b,t+1}) q^b_{b,t+1}\right) \end{array} \right\},$$

where $q^b_{m,t+1}$ and $q^b_{b,t+1}$ are the quantities of GM goods purchased with money and Bitcoin, respectively, in the next period. The real money price of $p_{m,t+1}$ is equal to $\phi_{t+1}\tilde{p}_{m,t+1}$ where $\tilde{p}_{m,t+1}$ is the unit price in money. Buyers take the aggregate miners' efforts, ME_{t+1}; the total quantity of GM goods traded with Bitcoin, $q_{b,t+1}$; and hence the discount factor $\delta(ME_{t+1}, q_{b,t+1})$ in period $t+1$ as given. Note that a buyer must pay additional $f q^b_{b,t+1}$ units of Bitcoin to miners as transaction fees in the GM in order to buy GM goods with Bitcoin.

Then, the first order conditions of the buyer's problem, assuming the interior solution, are

$$\frac{\phi_t}{\phi_{t+1}} p_{m,t+1} = \beta u'\left(q^b_{t+1}\right) \tag{4}$$

$$\frac{\psi_t}{\psi_{t+1}} p_{b,t+1}(1+f) = \beta \delta(ME_{t+1}, q_{b,t+1}) u'\left(q^b_{t+1}\right), \tag{5}$$

where $q^b_{t+1} = q^b_{m,t+1} + \delta(ME_{t+1}, q_{b,t+1}) q^b_{b,t+1}$. The left-hand side in (4) and (5) can be interpreted as the marginal cost of bringing one additional unit of money and Bitcoin to the GM, whereas the right-hand side can be the present value of the marginal benefit from increasing consumption in the GM by using the additional money or Bitcoin. Notice that we can derive an indifference condition between

money and Bitcoin in the steady state equilibrium by dividing (5) by (4):

$$\frac{\gamma_b(1+f)}{\delta(ME_{t+1}q_{b,t+1})}p_{b,t+1} = \gamma p_{m,t+1}.$$

This condition shows the relationship between the real money price, $p_{m,t+1}$, and the real Bitcoin price, $p_{b,t+1}$, of GM goods at which buyers will be indifferent to the choice between money and Bitcoin as an MOE in equilibrium.

Seller's problem As explained in Section 2, sellers are required to pay sales tax for money transactions, whereas there is no sales tax on Bitcoin transactions as in reality. Because sellers do not consume goods in the GM, sellers have no incentive to carry money and Bitcoin into the GM, given the condition that $\frac{\phi_t}{\phi_{t+1}} > \beta$ and $\frac{\psi_t}{\psi_{t+1}} > \beta$. Thus, the seller's problem in the CM of period t is written as

$$\underset{q^s_{m,t+1},q^s_{b,t+1}}{Max} \left\{ -c(q^s_{m,t+1}+q^s_{b,t+1}) + p_{m,t+1}(1-\tau_m)q^s_{m,t+1} + p_{b,t+1}q^s_{b,t+1} \right\},$$

where $\tau_m \in [0,1]$ is the sales tax rate for money transactions. Assuming that $q^s_{m,t+1}$ and $q^s_{b,t+1}$ are strictly positive, the first order conditions of the seller's problem are:

$$c'(q^s_{m,t+1}+q^s_{b,t+1}) = p_{m,t+1}(1-\tau_m) \tag{6}$$

$$c'(q^s_{m,t+1}+q^s_{b,t+1}) = p_{b,t+1}. \tag{7}$$

(6) and (7) presents that the marginal cost of producing GM goods for money and Bitcoin, respectively, must be equal to the marginal benefit from selling them. $p_{m,t+1}(1-\tau_m)$ represents the after-tax real income from selling one unit of GM

goods in exchange of money and $p_{b,t+1}$ stands for real income from selling GM goods in exchange of Bitcoin. Lastly, dividing (6) by (7) yields an indifference condition between money and Bitcoin for sellers as follows.

$$p_{b,t+1} = p_{m,t+1}(1-\tau_m) \tag{8}$$

As in the above buyers' case, in equilibrium, sellers must be indifferent to the choice between money and Bitcoin as an MOE in the GM.

4 Equilibrium

We construct stationary equilibria with coexistence of money and Bitcoin where all real variables are constant over time. Stationarity implies $\phi_t M_t = \phi_{t+1} M_{t+1}$ and $\psi_t B_t = \psi_{t+1} B_{t+1}$, which means that $\gamma = \frac{\phi_t}{\phi_{t+1}}$ and $\gamma_b = \frac{\psi_t}{\psi_{t+1}}$. Moreover, we restrict our attention to equilibria where γ and γ_b are strictly higher than the discount rate β because, otherwise, an equilibrium does not exist.

Our definition of equilibrium is standard. Given prices, all agents behave optimally, all markets clear, and the government budget constraint is balanced in equilibrium, as described in the next definition.

Definition 1 *A steady state equilibrium is a lis,t* $\{z, z_b, q_m^b, q_b^b, q_m^s, q_b^s, q_m, q_b, p_m, p_b, \tau\}$, *where* $z \equiv \phi_t M_t$ *and* $z_b \equiv \psi_t B_t$, *such that:*

1. *Given* $\{p_m,\ p_b,\ \gamma,\ \gamma_b,\ ME, q_b\}$, $\{q_m^b, q_b^b\}$ *solves the buyer's problem;*

2. *Given* $\{p_m,\ p_b\}$, $\{q_m^s, q_b^s\}$ *solves the seller's problem;*

3. *Given* $\{\gamma_b, z_b, p_b, q_b, ME\}$, $\{e\}$ *solves the miner's problem and miners optimally decide whether to enter to the mining work or not;*

4. *The Buyers' demand for GM goods that are purchased with money and Bitcoin, respectively, must equal the supply by sellers in the GM:*

$$q_m^b = q_m^s \equiv q_m \tag{9}$$

$$q_b^b = q_b^s \equiv q_b \tag{10}$$

5. *Currency markets for money and Bitcoin must clear in the CM:*

$$z = \gamma p_m q_m \tag{11}$$

$$z_b = \gamma_b \left[p_b q_b (1+f) \right] \tag{12}$$

6. *The government (a consolidated authority) budget constraint (1) is satisfied.*

To characterize equilibrium, we substitute (2) into (3), and obtain the following equation, using the fact that $ME = \eta e$ in equilibrium.

$$\beta [e\upsilon'(e) - \upsilon(e)] = k, \tag{13}$$

which uniquely determines e given our functional assumption on $\upsilon(e)$, and each miner's effort e increase with respect to k. Thus, each miner's efforts only depend on the entry cost k and not on other economic variables, such as Bitcoin price and transaction fees. However, this does not mean that the aggregate mining effort, ME, is fixed because the mass of active miners η depends on other economic conditions.

Next, from (4), (5), (6), and (7), we obtain

$$\frac{\gamma_b(1+f)(1-\tau_m)}{\gamma} = \delta(ME, q_b) \tag{14}$$

Because $\delta(ME, q_b) \in [0,1]$, the necessary condition for equilibrium to exist is $\gamma_b(1+f)(1-\tau_m) \leq \gamma$, which is emphasized in the following proposition.

Proposition 1 *The necessary condition for the coexistence of money and Bitcoin is* $\gamma_b(1+f)(1-\tau_m) \leq \gamma$

Proposition 1 implies that the inflation rate, γ, must be sufficiently high for money and Bitcoin to coexist in equilibrium, where buyers and sellers must be indifferent to the choice between money and Bitcoin. An increase in Bitcoin growth rate, γ_b, or the transaction fees, f, makes Bitcoin less attractive as a medium of exchanges. To make Bitcoin and money indifferent from the other, the money holding cost—that is, inflation—should rise. Similarly, as sales tax, τ_m, increases, γ must fall to allow money to be held in equilibrium.

Note, however, that Proposition 1 states the necessary condition for money and Bitcoin to coexist as an MOE in equilibrium. It does not mean that Bitcoin cannot be used as MOE if this necessary condition is not satisfied. In a money search model, it is always a feasible equilibrium in which fiat currency is not valued. Thus, if money is not used as an MOE so $\phi_t = 0$ for all t, then Bitcoin can be used as an MOE with positive value in equilibrium, even if the condition in Proposition 1 is violated.

Now we can express q_b and η as a function of p_m by combining and re-arranging

(2), (5), (6), (7), (9), (10), (12), (14), and the equilibrium condition, $ME = \eta e$, as

$$(15)\quad q_b = \widehat{q}_b(p_m) \equiv \frac{\gamma}{\gamma - \gamma_b(1+f)(1-\tau_m)} \left\{ c'^{-1}\left(p_m(1-\tau_m)\right) - u'^{-1}\left(\frac{\gamma p_m}{\beta}\right) \right\}$$

$$(16)\quad \eta = \widehat{\eta}(p_m) \equiv \frac{(1-\tau_m)\left[\gamma_b(1+f)-1\right] p_m \widehat{q}_b(p_m)}{e\upsilon'(e)},$$

where the miner's effort, e, are given by (13). Then, by substituting (15) and (16) into (14), we obtain the following equation.

$$(17)\qquad \frac{\gamma_b(1+f)(1-\tau_m)}{\gamma} = \delta\left(\widehat{\eta}(p_m)e, \widehat{q}_b(p_m)\right)$$

This allows us to obtain the equilibrium value of p_m, given which, we can obtain the value for p_b, q_m, q_b, η, τ from (1), (6), (7), (11), (15), and (16), which characterizes the whole equilibrium.

In general, we cannot characterize equilibrium analytically, but we can obtain economic intuitions about the mechanism through which monetary policy affects the model economy by making a simplifying assumption. As we explained in the introduction, the current Bitcoin system is programmed such that it takes 10 minutes, on average, to mine a new block. This implies that the aggregate mining effort, ME, does not critically affect the waiting time until a Bitcoin transaction is confirmed by mining work, although it still has some effects. Based on this rationale, we assume for a moment that the aggregate mining effort ME does not affect the discount factor δ. Thus, δ is a function of q_b only, and we further assume that $[q_b\delta(q_b)]' \geq 0$.

Now we analyze the effects of monetary policy on the economy. Given the sim-

plifying assumption that δ is a function of q_b only, the equilibrium condition (17) uniquely determines the aggregate quantity of GM goods, q_b, traded with Bitcoin as $q_b = \delta^{-1}\left(\frac{\gamma_b(1+f)(1-\tau_m)}{\gamma}\right)$. Thus, as the inflation rate, γ, increases, q_b rises. The effects of changing γ on p_m and η, which are determined by (15) and (16), respectively, are unclear because the sign of the partial derivative of the right-hand side of (15) with respect to γ is not evident. It depends on the functional form of $c(\cdot)$ and $u(\cdot)$. Next, from (6), (15), and (17), we obtain

$$q_m = u'^{-1}\left(\frac{\gamma p_m}{\beta}\right) - q_b\delta(q_b).$$

Thus, if p_m rises when γ increases, q_m must fall given the assumption that $[q_b\delta(q_b)]' \geq 0$. On the other hand, if p_m decreases when γ increases, then $q_m = c'^{-1}(p_m(1-\tau_m)) - q_b$ must also fall because q_b increases with respect to γ. Combined together, q_m falls when γ increases; hence, the ratio of the quantity of GM goods traded with Bitcoin to the aggregate GM goods production, $\frac{q_b}{q_m+q_b}$, rises. This is intuitive because an increase in γ indicates an increase in the money holding cost. Hence, money becomes less attractive to buyers as an MOE. Thus, buyers trade more GM goods with Bitcoin and fewer GM goods with money.

Next suppose the Bitcoin transaction fees, f, increase. Then, $q_b = \delta^{-1}\left(\frac{\gamma_b(1+f)(1-\tau_m)}{\gamma}\right)$ decreases, which is intuitive because buyers have to pay more transaction fees to purchase GM goods with Bitcoin. An unintuitive part is that the price of GM goods in terms of real money, p_m, falls as f rises according to the equilibrium condition (15). It seems to be unintuitive, but its economic intuition is as follows. As transaction fees, f, rise, the price of GM goods in terms of real Bitcoin, p_b, must fall for

Bitcoin to be used as an MOE in equilibrium. Then, the price of GM goods in terms of real money, p_m, must also fall because of the seller's indifference condition (8) for money and Bitcoin. Finally, an increase in f has a direct effect on the active miner mass η in addition to the indirect effect through p_m and q_b; it is, however, not evident whether η (hence, the aggregate mining effort, $ME = \eta e$) increases or decreases.

5 Quantitative Analysis

We now study the effects of monetary policy quantitatively in an economy where money and Bitcoin coexist in equilibrium. Here, we emphasize that we analyze deterministic transitions across steady state equilibria, and not a business cycle. In particular, we study how an increase in money growth rate and changing transaction fees affects trading volume with each type of currency, prices, and welfare. To study the implication on welfare, we define the sum of expected utilities in a steady state equilibrium across agents. In particular, our welfare measure is given by:

$$W = u(q_m + \delta(ME, q_b)q_b) - c(q_m + q_b) - \omega\eta\left[\upsilon(e) + \beta k\right] - g - \theta p_m q_m \tag{18}$$

where $\omega \in [0,1]$ represents the proportion of domestic miners to all miners in the world. More precisely, verification of a Bitcoin transaction can be done by any miner outside of a domestic country. For example, a miner in China can verify a Bitcoin transaction in the U.S. by adding a new block to the blockchain. Since we are interested in welfare of a domestic economy, we subtract only ω fraction of welfare cost from mining work—disutility from the mining efforts and the entry cost.

Therefore, if all mining work is done by foreign miners, then ω would be zero, for instance, and there is no welfare loss of domestic economy from the mining. Note that a miner must pay the entry cost k in the previous CM, and so it is discounted in (18). Finally, we subtract government expenditure and cash management cost as welfare loss.

5.1 Calibration

The functional forms are standard. The *DM* utility and cost functions are $u(q) = \frac{(q+\varepsilon)^{1-\alpha}-\varepsilon^{1-\alpha}}{1-\alpha}$ and $c(h) = h^{\sigma}$ where $\varepsilon \approx 0$. Miners' disutility function from efforts is $\upsilon(e) = e^{\rho}$ and the discount factor for Bitcoin transactions is $\delta(ME, q_b) = \frac{ME}{(\delta_1+ME)(1+\delta_2 q_b)}$. We let the time period be a year, and set $\beta = 0.97$, where the annual real interest rate on an illiquid bond is 3.09%. We set $\gamma = 1.02$, such that the inflation rate in a steady state reflects the Federal Reserve System's inflation target. The estimates of curvature of $u(q)$ vary widely, but we use $\alpha = 1.5$ within the range of previous studies. Typical monetary theory literature often assumes the linear production technology in the *DM*, and also previous studies on cryptocurrency, such as Chiu and Koeppl (2017), often used a linear disutility function for miner's efforts for tractability. Then, however, Walrasian price, p_b, trivially corresponds to seller's marginal production cost in the *DM*, and a linear function for miner's disutility from effort is not compatible with endogenizing the miners' mass with the entry cost $k > 0$ in our model. For these reasons, we use strictly convex functions for $c(h)$ and $\upsilon(e)$, and set $\sigma = \rho = 2$.[14]

[14]However, the main implications of the model do not change with other values for σ and ρ as long as we calibrate the rest of our parameters appropriately.

Next, δ_1 influences the effects of aggregate miners' efforts, ME, on the discount factor $\delta(ME, q_b)$. In principle, ME affects the time to finish PoW for adding a new block to the blockchain. However, in reality, the technical structure of Bitcoin was invented such that the average time to compute a hash value to mine a new block would be 10 minutes. This implies that the miners' efforts, ME, do not dramatically affect the time for mining a new block and, hence, the discount factor, $\delta(ME, q_b)$, although it still has some minor effects. Thus, we set δ_1 sufficiently small as $\delta_1 = 0.00001$. However, the aggregate quantity of Bitcoin transactions has a meaningful effect on the time of confirming a particular transaction. This is because, if there are multiple blocks which are mined almost at the same time, each block is added to the blockchain in order, and a transaction that is contained in the last block will be confirmed at the end. As the Bitcoin transaction volume increases, more blocks need to be created. Thus, the average time to confirm a particular transaction increases. To reflect this fact, we calibrate δ_2 from the data as below. We use the aggregate Bitcoin transactions data, cash management cost, the estimated number of active miners, federal government expenditure, monetary base, and sales tax rates, to calibrate the remaining parameters (see Table 1). We use data spanning a period from 2016 to 2017, because the data, such as Bitcoin growth rate, transaction volume, and fees before 2016, are unstable. We set $f = 0.0007$ to match the ratio of the transaction fees to the Bitcoin transaction volume. The average annual growth rate of the Bitcoin stock is 5.7%, that is, $\gamma_b = 1.057$. We choose $\delta_2 = 4$ to target the ratio of the value of the Bitcoin stock in terms of U.S. dollar to the monetary base in the U.S., as $\frac{\psi_t B_t}{\phi_t M_t} \approx 0.00997$.[15] Although data for the

[15] From (17), $q_b \approx \frac{1}{\delta_2}\left\{\frac{\gamma}{\gamma_b(1+f)(1-\tau_m)} - 1\right\}$, given $\delta_1 \approx 0$. Then, δ_2 has a first order effect on q_b and

number of active miners in the world does not exist, an estimate shows that there are likely to be over 1,000,000 unique individuals mining bitcoins.[16] We use one million as an estimate of active miners, and set $k = 0.0454$ to match the ratio of number of active miners in the world to the average population of households in the U.S, as $\frac{\eta}{2} \approx 0.00316 = 1,000,000/316,418,191$. We use the average sales tax rates across all states in the U.S., and set $\tau_m = 0.067$. The payment system data from the Federal Reserve System indicates that the average cash management cost in 2016-2017 in the U.S. is \$1.246 billion, and we set $\theta = 0.00013$ to target the ratio of cash management cost to GDP for the same period.[17] Finally, we choose $g = 0.4789$ to match the ratio of federal government expenditure to GDP.

5.2 Quantitative results

We now turn to the quantitative evaluation of the effects of monetary policy and Bitcoin transaction fees (or Bitcoin growth rate) on economic activities and welfare. Figure 1 shows steady state values for the macro economic variables as a function of money growth rate, γ, from 1 to 1.6 (in terms of the inflation rate, from 0% to 60%). Higher inflation indicates higher money holding cost, and thus the quantity of GM goods traded with money decreases as inflation increases similar to the standard monetary theory. Instead, more GM goods are traded with Bitcoin because

the ratio of Bitcoin stock to money stock, defined as $\frac{\psi_t B_t}{\phi_t M_t} = \frac{\gamma_b p_b q_b (1+f)}{\gamma(p_m q_m + m^s)}$, in a steady state equilibrium.

[16] See Buy Bitcoin World (https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there)

[17] Cash management cost includes printing new currency, transportation, destruction of mutilated currency, and Federal Reserve expenses for cash operations.

Parameters and definition		Values	Identified	Data	Model
β	Discount factor	0.97	Set directly	-	-
γ	Money growth rate	1.02	”	-	-
α	Curvature of $u(q)$	1.5	”	-	-
σ	Curvature of $c(h)$	2	”	-	-
ρ	Curvature of $\upsilon(e)$	2	”	-	-
δ_1	Coefficient on ME in $\delta(ME,q_b)$	0.00001	”	-	-
f	Bitcoin transaction fee	0.0007	Transaction fee/trade volume	0.0007	0.0007
γ_b	Bitcoin growth rate	1.057	Bitcoin growth rate	1.057	1.057
δ_2	Coefficient on $q_b$in $\delta(ME,q_b)$	4	Bitcoin stock/monetary base	0.00997	0.0096
k	Entry cost of miners	0.0454	# of miners/population	0.0032	0.0032
τ_m	Sales tax rate	0.067	Sales tax rates in the U.S.	0.067	0.067
θ	Marginal cash management cost	0.00013	Cash management cost/GDP	0.00007	0.00007
g	Government expenditure	0.4789	Federal gov. expenditure/GDP	0.2234	0.2234

Table 1: Calibration

of the substitution effect caused by changes in the relative holding cost. In particular, the ratio of the quantity of GM goods traded with Bitcoin to the aggregate GM goods production, $\frac{q_b}{q_m+q_b}$, rises from around 0.16% to 24.6%. The increase in Bitcoin transactions leads to an increase in the aggregate transaction fees, which attract more miners into the mining competition. As a result, the aggregate mining effort, ME, also increases. The real money price of GM goods, p_m, decreases to compensate for the increase in money holding cost. The real Bitcoin price of GM goods, p_b, also decreases because sellers supply more GM goods for Bitcoin. In equilibrium, $p_b = p_m(1-\tau_m)$. An increasing γ has two counteracting effects on the lump-sum taxes, τ. First, because the real value of money transaction, $p_m q_m$, falls, the government net revenue from operating money, $(\tau_m - \theta)p_m q_m$, decreases. Second, as γ rises, however, the government income from seigniorage increases. The second effect dominates the first one, and hence the lump-sum taxes, τ, falls to

balance government budget.

In the last panel of Figure 1, we compare the aggregate trade volume, the effective consumption, and the welfare between an equilibrium where money and Bitcoin coexist (coexistence equilibrium) and an equilibrium where only money is traded as a medium of exchanges (money-only equilibrium).[18] First, the aggregate trade volume in the GM, $(q_m + q_b)$, decreases in both cases as inflation increases because the increased money holding cost decreases more q_m than it increases q_b. As a result, the total trade volume is higher in the coexistence equilibrium than in the money-only equilibrium, and the gap between them increases as inflation increases. This is because, as inflation increases, the money holding cost increases, and thus buyers trade fewer GM goods with money. However, when Bitcoin can also be used as an MOE in transactions, buyers can pay Bitcoin instead of money in exchange for GM goods. Thus, the decrease in the quantity of the aggregate trade is lower in the coexistence equilibrium than in the money-only equilibrium, as inflation rises. However, as the aggregate Bitcoin trade volume continues to increase, the average waiting time until a particular Bitcoin transaction is confirmed in the Bitcoin system increases. The increasing waiting time leads to a decrease in the discount factor $\delta(ME, q_b)$, and consequently, in the effective consumption, $q_m + \delta(ME, q_b)q_b$ at the end. In summary, more GM goods are produced in the coexistence economy than in a money-only economy. However, buyers enjoy less utility from GM goods consumption because of the increased waiting time for confirming Bitcoin transactions. Accordingly, the overall welfare is lower in the coexistence economy

[18] In an equilibrium where money is the only MOE, the aggregate production and consumption of GM goods are given by q_m because $q_b = 0$. In this case, we have the same equilibrium results as in Lagos and Rocheteau (2008).

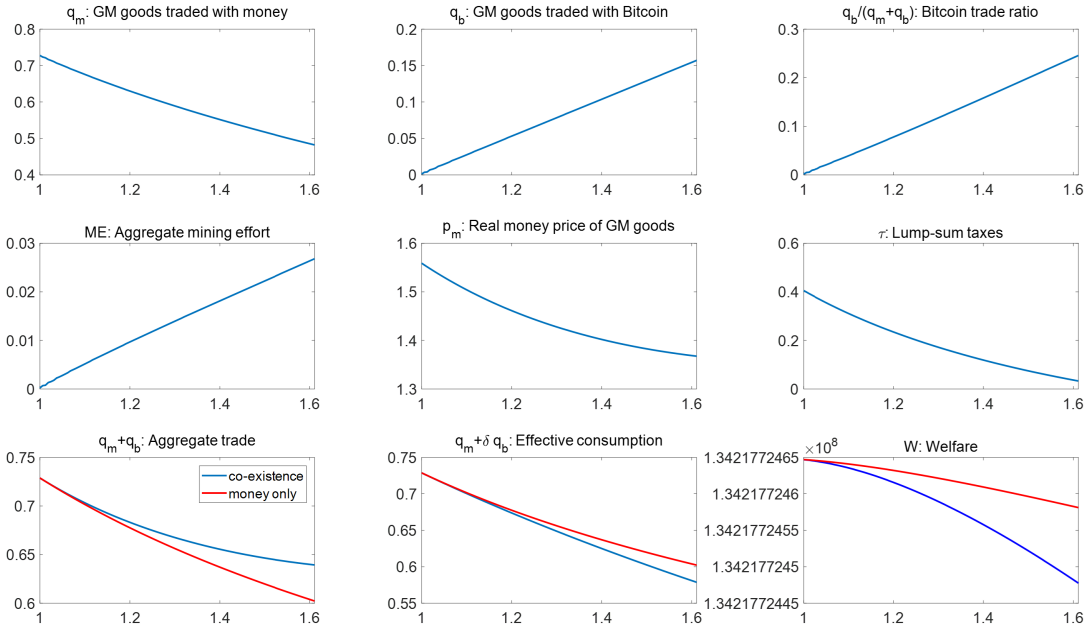

Figure 1: Money growth rate, γ, and aggregate variables

than in the money-only economy. Moreover, the welfare gap increases as inflation increases.[19]

We now study how an increase in the transaction fees, f (or the growth rate of Bitcoin stock, γ_b), affects economic activities and welfare. In a steady-state equilibrium, an increase in f has exactly the same effect as an increase in γ_b. Thus, we focus on the effects of changing f from zero to 0.5. As described in the Proposition 1, if the transaction fees are high, then the money growth rate, γ, must be sufficiently high for money and Bitcoin to coexist. Thus, we set $\gamma = 1.5$ in the following analysis. However, the main qualitative implication does not hinge on this value on γ. If γ is small, then the upper-bound of f should be low enough; otherwise, there is no meaningful change.

[19]For welfare analysis, we set $\omega = 0.5$, but the main result is robust for all $\omega \in [0,1]$.

Figure 2 describes the effects of the Bitcoin transaction fees on aggregate economic activities and welfare. Intuitively, as the transaction fees increase, buyers use more money as an MOE to trade GM goods (see the first panel of Figure 2). An increase in f pushes down the real Bitcoin price of GM goods, p_b, pushing buyers to use Bitcoin as an MOE in equilibrium. Hence, p_m also falls, given the equilibrium condition that $p_b = p_m(1-\tau_m)$. The aggregate mining effort, ME, shows a hump shape because, intuitively, when f is low, an increase in f raises the real value of the aggregate transaction fees, $F = f p_b q_b$, although the real value of the Bitcoin trade volume, $p_b q_b$, decreases in equilibrium, attracting more miners into the mining game. However, once f is sufficiently high, then its negative effects on F through a decrease in the real value of the Bitcoin trade volume, $p_b q_b$, dominates the positive effect on F. Hence, the miners' mass falls and the aggregate mining effort, ME, decreases. Next, because an increase in q_m dominates a decrease in p_m, the real value of money transaction, $p_m q_m$, increases, which raises government net revenue from operating money, $(\tau_m - \theta) p_m q_m$, and seigniorage by raising the real value of money stock, $z = \gamma p_m q_m$. Thus, the lump-sum tax τ, that balances government budget, falls. The last panel shows the effects of the transaction fees on the aggregate trade volume, effective consumption, and welfare. Although an increase in q_m partially substitutes for a decrease in q_b, the aggregate trade volume, $(q_m + q_b)$, decreases as the transaction fees, f, increase. However, as the Bitcoin transactions, q_b, decrease, the average waiting time for the confirmation of Bitcoin transactions decreases, and thus $\delta(ME, q_b)$ increases. Consequently, the effective consumption, $q_m + \delta(ME, q_b) q_b$, of buyers increases, and the welfare also increases.

Now, we study the economy where Bitcoin is the only MOE, or the Bitcoin-

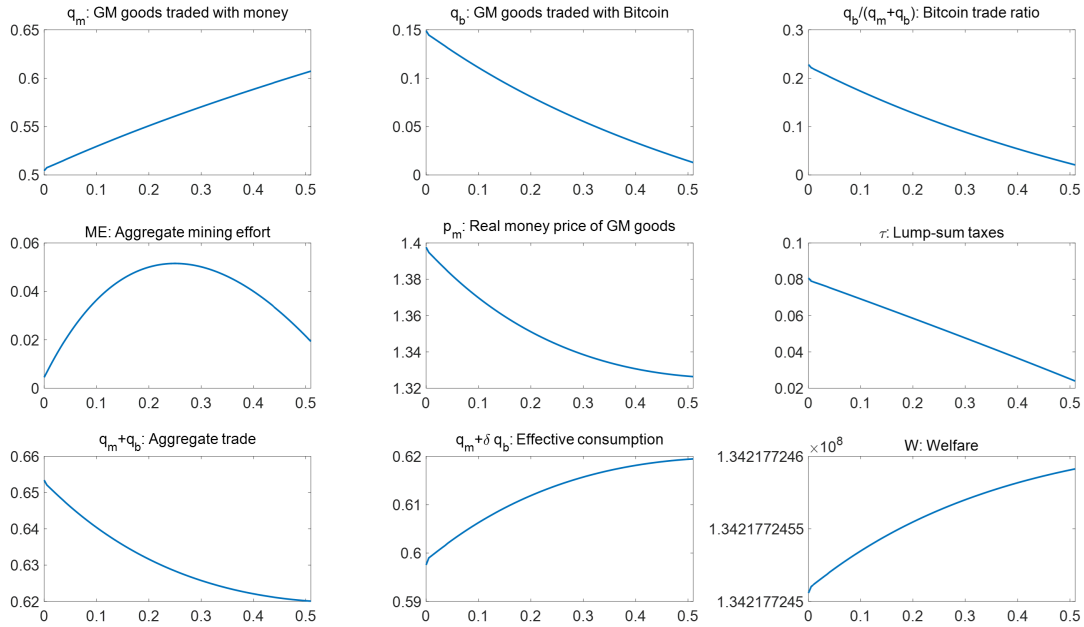

Figure 2: Bitcoin transaction fee, f, and aggregate variables

only economy, which is similar to other cryptocurrency literature, such as Chiu and Koeppl (2017).[20] This allows us to better understand the effects of the transaction fees on economic activities and welfare. Figure 3 describes the effects of f in the Bitcoin-only economy. An increase in f means an increase in the transaction cost in the GM, and thus the buyers' demand for GM goods decreases. The trade volume of GM goods, q_b, decreases, and the price, p_b, falls as an equilibrium outcome. The aggregate miners' mass and the mining efforts increase because f increases the aggregate reward to miners. A key difference from the baseline model in which money and Bitcoin coexist is that welfare decreases as the transaction fee increases, similar to the policy implication presented in Chiu and Koeppl (2017). This is

[20] In an equilibrium where Bitcoin is the only MOE, the aggregate production and consumption of GM goods are represented by q_b because $q_m = 0$ (See Appendix for the characterization of equilibrium with Bitcoin only).

because the transaction fees exactly have the same effect that the money holding cost, such as inflation, has in a standard money search model, thereby reducing the trade volume in the GM inefficiently. In particular, although a decrease in q_b and an increase in ME improves $\delta(ME, q_b)$, a decrease in q_b dominates an increase in $\delta(ME, q_b)$. Hence, the effective buyer's consumption $\delta(ME, q_b)q_b$ falls. Further, an increase in the aggregate mining efforts, ME, reduces welfare as long as ω is strictly positive.

When money and Bitcoin coexist as in our baseline model, buyers can substitute Bitcoin into money in the GM good transactions. Hence, the aggregate exchanges in the GM decrease less compared with the Bitcoin-only economy. More precisely, as the transaction fees rise from zero to 0.5, the aggregate trading volume in the Bitcoin-only economy decreases by 17.8%, but the trading volume in the coexistence economy decreases only by 5.1%. Moreover, money is a more efficient MOE than Bitcoin because of the discount factor, $\delta(ME, q_b)$, for Bitcoin transactions, unless the cash management cost, θ, is unrealistically high in the coexistence economy. Bitcoin can become more efficient as an MOE, as the Bitcoin trading volume, q_b, decreases, and thus $\delta(ME, q_b)$ increases. Consequently, switching from Bitcoin to money improves welfare. Welfare increases as the transaction fees increase in the baseline model where money and Bitcoin coexist.

6 Conclusion

Our study shows how central bank-issued money and a cryptocurrency, Bitcoin, compete as an MOE and whether or not monetary policy and the main features of

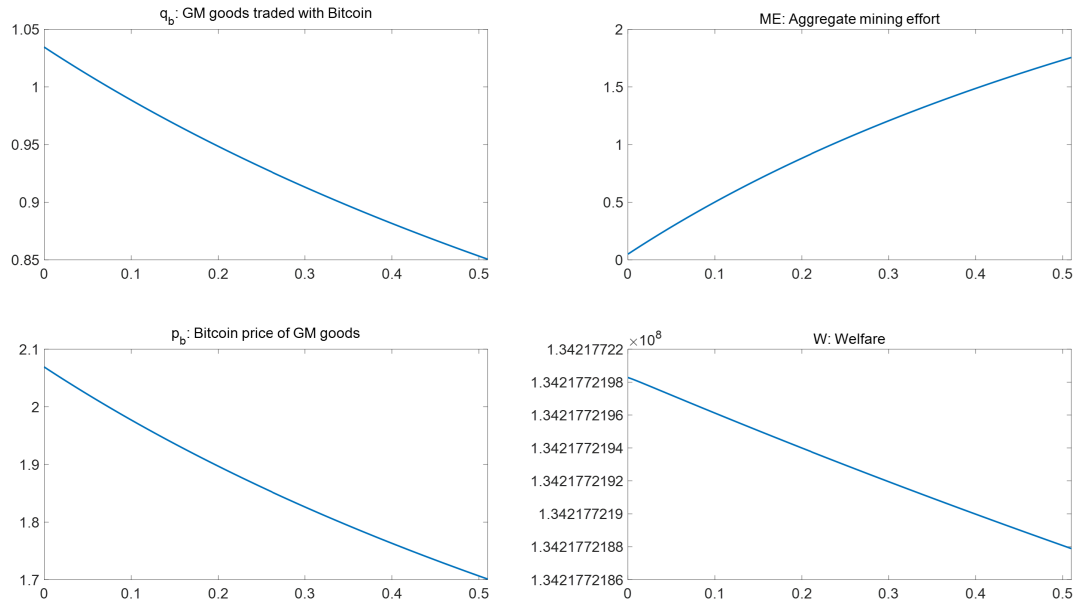

Figure 3: The effects of marginal Bitcoin transaction fee, f, in an economy where Bitcoin is the only MOE

the current Bitcoin system, such as transaction fees, affect economic activities and welfare. Interestingly, our quantitative analysis demonstrates that Bitcoin can effectively compete with money only when the inflation rate is sufficiently high, considering the current Bitcoin system. Furthermore, economic welfare in the money-only economy is higher than that in the coexistence economy. As the inflation rate increases, the money-only economy accomplishes a strictly higher level of welfare than the coexistence economy. The lower welfare in the coexistence economy is primarily attributed to inefficient mining processes in the current Bitcoin system. The size of a new block that can be added to the existing blockchain is fixed at most at 1 MB. This limits the number of Bitcoin transactions processed at once. As the volume of transactions where Bitcoin is used as an MOE increases, the limited size of a new block implies that more time is required, on average, until a new

Bitcoin transaction is validated and recorded in the Bitcoin ledger. As the inflation rate increases, the required time increases, because money is substituted for Bitcoin, which increases Bitcoin transactions. Consequently, the delayed time for validation and recording lowers effective consumption. Thus welfare losses in the coexistence economy occur, even if the actual trade volume is greater. Lastly, the welfare increases with transaction fees because an increase in the latter leads to more money transactions, which is more efficient as an MOE, but to fewer Bitcoin transactions. On the other hand, in a Bitcoin-only economy, economic welfare can be maximized by minimizing transaction fees which reduce the trade volume of goods inefficiently.

The competition between money and blockchain technology based cryptocurrencies still requires extensive research, because the technical structure of cryptocurrencies is totally different from that of the existing digitalized currencies which are built on the centralized ledgers. Among others, it would be interesting to introduce an alternative mining protocol, such as Proof of Stake, to improve efficiency of such currencies as an MOE. As shown in Chiu and Koeppl (2017), the mining protocol of PoW in the present Bitcoin system is one of the main causes for Bitcoin's inefficiency compared with money as an MOE, which causes welfare losses when Bitcoin is widely used as an MOE. Also, this study helps to examine how a blockchain-based cyrptocurrency in an economy with money should be designed to improve economic welfare, and furthermore how the current money system can adapt to technological progress by including blockchain technology. More precisely, it would benefit our understanding of cryptocurrencies to investigate the optimal structure of the Central Bank Digital Currency which may be newly issued in

the near future.

References

BERENTSEN, A. AND F. SCHAR (2018): "A Short Introduction to the World of Cryptocurrencies," *Review*, 100, 1–16.

CAVALCANTI, R. D. O. AND N. WALLACE (1999): "Inside and Outside Money as Alternative Media of Exchange," *Journal of Money, Credit and Banking*, 31, 443–457.

CHIU, J. AND T. KOEPPL (2017): "The Economics of Cryptocurrencies - Bitcoin and Beyond," Working Papers 1389, Queen's University, Department of Economics.

CHIU, J. AND T.-N. WONG (2015): "On the essentiality of e-money," Bank of Canada Staff Working Paper 2015-43, Ottawa.

CONG, L. W., Y. LI, AND N. WANG (2018): "Tokenomics: Dynamic Adoption and Valuation," Working paper series, Ohio State University, Charles A. Dice Center for Research in Financial Economics.

DIAMOND, D. W. AND P. H. DYBVIG (1983): "Bank Runs, Deposit Insurance, and Liquidity," *Journal of Political Economy*, 91, 401–419.

FERNÁNDEZ-VILLAVERDE, J. AND D. SANCHES (2016): "Can Currency Competition Work?" NBER Working Papers 22157, National Bureau of Economic Research, Inc.

GANDAL, N. AND H. HALABURDA (2014): "Competition in the Cryptocurrency Market," Working Papers 14-17, NET Institute.

GANDAL, N., J. HAMRICK, T. MOORE, AND T. OBERMAN (2017): "Price Manipulation in the Bitcoin Ecosystem," CEPR Discussion Papers 12061, C.E.P.R. Discussion Papers.

GLASER, F., M. HAFERKORN, M. WEBER, AND K. ZIMMERMANN (2014): "How to price a Digital Currency? Empirical Insights on the Influence of Media Coverage on the Bitcoin Bubble," *Banking and information technology*, 15, 1404–1416.

KOCHERLAKOTA, N. AND N. WALLACE (1998): "Incomplete Record-Keeping and Optimal Payment Arrangements," *Journal of Economic Theory*, 81, 272 – 289.

KOCHERLAKOTA, N. R. (1998): "Money Is Memory," *Journal of Economic Theory*, 81, 232 – 251.

LAGOS, R. AND G. ROCHETEAU (2008): "Money and capital as competing media of exchange," *Journal of Economic Theory*, 142, 247–258.

LAGOS, R. AND R. WRIGHT (2005): "A Unified Framework for Monetary Theory and Policy Analysis," *Journal of Political Economy*, 113, 463–484.

NAKAMOTO, S. (2009): "Bitcoin: A peer-to-peer electronic cash system," *http://bitcoin.org*.

OUATTARA, H. F., D. AHMAT, F. T. OUÉDRAOGO, T. F. BISSYANDÉ, AND O. SIÉ (2018): "Blockchain Consensus Protocols," in *e-Infrastructure and e-Services for Developing Countries*, ed. by V. Odumuyiwa, O. Adegboyega, and C. Uwadia, Cham: Springer International Publishing, 304–314.

ROCHETEAU, G. AND R. WRIGHT (2005): "Money in search equilibrium, in competitive equilibrium, and in competitive search equilibrium," *Econometrica*, 73, 175–202.

ROUTLEDGE, B. AND A. ZETLIN-JONES (2018): "Currency Stability Using Blockchain Technology," 2018 Meeting Papers 1160, Society for Economic Dynamics.

Appendix A: Bitcoin-only economy

In this appendix, we study the economy in which Bitcoin is the only medium of exchanges, so $q_m = 0$. Because there is no any variables related to money in the miner's problem in the baseline model, the miner's problem and miner's optimal choices do not change. However, there are minor changes in other agents' problem because $q_m = 0$ in this economy.

First, the buyer now must decide Bitcoin balance holding and the quantity of GM goods. Then, in the steady state, the buyer's problem is

$$\underset{q_b^b}{Max}\left\{-\gamma_b p_b(1+f)q_b^b + \beta u\left(\delta(ME,q_b)q_b^b\right)\right\}$$

which yields

$$\gamma_b p_b(1+f) = \beta\delta(ME,q_b)u'\left(\delta(ME,q_b)q_b^b\right) \tag{19}$$

as the first order condition.

Next, since we assume that government imposes sales tax on money trade only in the GM, the seller does not need to pay sales tax in the Bitcoin-only economy. Thus, the seller's problem is

$$\underset{q_b^s}{Max}\{-c(q_b^s) + p_b q_b^s - \tau\}$$

which gives us

$$c'(q_b^s) = p_b \tag{20}$$

as the first order condition.

The market clearing conditions are

$$q_b^b = q_b^s = q_b \tag{21}$$

$$z_b = \gamma_b p_b q_b (1+f), \tag{22}$$

where $z_b = \psi_t B_t$.

Then, from (2), (13), and (20) - (22), we can express η as a function of q_b as

$$\eta = \widehat{\eta}_b(q_b) \equiv \frac{c'(q_b) q_b [\gamma_b (1+f) - 1]}{e \upsilon'(e)}. \tag{23}$$

Then, substituting (20) - (21), and (23) into (19), we obtain

$$\gamma_b c'(q_b)(1+f) = \beta \delta(\widehat{\eta}_b(q_b) e, q_b) u'(\delta(\widehat{\eta}_b(q_b) e, q_b) q_b),$$

which gives the equilibrium value of q_b. Then, we can obtain the value for p_b and η from (20) and (23), and $\tau = g$ by (1).