Money, Cryptocurrency, and Monetary Policy

Kee-Youn Kang[†]   Seungduck Lee[‡]

June 11, 2019

Abstract

We develop a search theoretic model in which both money and Bitcoin can be used as a medium of exchange, and currency choices are determined endogenously. We analytically study the conditions necessary for the coexistence of money and Bitcoin in equilibrium, and its effects on welfare. The results of our quantitative analysis show that Bitcoin can compete meaningfully with money only when the inflation rate is sufficiently high, and that welfare in an economy with both money and Bitcoin is lower than that in a money-only economy, due to Bitcoin's inefficient mining process. The welfare gap between the two economies expands as the inflation rate increases. An increase in Bitcoin transaction fees can increase welfare by reducing inefficient Bitcoin transactions.

JEL Classification: E31, E50, E52, G12

Keywords: Money, Cryptocurrency, Bitcoin, Double-spending, Blockchain, Monetary Policy

---

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

We are grateful to David Andolfatto, Jonathan Chiu, Kyu-Hwan Cho, Athanasios Geromichalos, Lucas Herrenbrueck, Timothy Kam, Dongheon Kim, Yong-Gu Kim, Young Sik Kim, Dirk Niepelt, Cheolbeom Park, Jaevin Park, Joon Song, Hyunduk Suh, Sylvia Xiaolin Xiao, Christopher Waller, and Chien-Chiang Wang for their useful comments and suggestions, and Jong-Ik Park for data work. We would also like to thank the participants at the talks at KAIST Business School, Korea International Economic Association, Korea University, Korean Economic Association, SNB-CIF Conference on Cryptoassets and Financial Innovation, Sungkyunkwan University, the Bank of Korea, and Yonsei University. This research 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

Blockchain-based cryptocurrencies (e.g., Bitcoin) became popular in 2017, when the transaction volume and market capitalization increased remarkably.[1] This increase in public attention has led to a growing body of literature on cryptocurrencies, and intensive research in central banks.[2] However, our understanding of cryptocurrencies, particularly as a medium of exchange (henceforth, MOE), is still limited. Among others, this study attempts to answer the following questions: Can a cryptocurrency, Bitcoin, coexist or compete with central bank-issued money as an MOE? If so, how does monetary policy affect their coexistence and competition? Further, how do this policy and Bitcoin transaction fees affect cryptocurrency-related activities, such as the trade volume of cryptocurrency and economic welfare? Does the coexistence of money and Bitcoin improve economic welfare?

To address the above questions, we develop a monetary search model in which the central bank-issued fiat money (henceforth, *money*) and a cryptocurrency are used as an MOE.[3] In particular, we incorporate technical features of Bitcoin, a representative blockchain-based cryptocurrency, into the Lagos and Wright (2005) framework. We chose Bitcoin because it was the first major cryptocurrency, and it is the top-ranked cryptocurrency built on blockchain technology in terms of the market capitalization and trade volume. Furthermore, alternative cryptocurrencies, such as Bitcoin Cash, share most of the technological elements of Bitcoin. In reality, it is true that the term "Bitcoin" is widely used to represent a cryptocurrency,

[1] According to Coinlore, the market capitalization and daily trade volume of Bitcoin amount to \$112 billion and \$5 billion, respectively, as of September 21, 2018. (source: https://www.coinlore.com) Moreover, the dollar price of one Bitcoin (BTC) recorded an all-time high of \$19,783.06 on December 17, 2017 (source: https://www.blockchain.com).

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

[3] A general discussion of a monetary search model is available in Williamson and Wright (2010) and Lagos et al. (2017), and a textbook treatment can be found in Nosal and Rocheteau (2011).

and that the terms are oftentimes used interchangeably. Furthermore, the Lagos and Wright (2005) framework is well suited and tractable to incorporate the distinctive technological features of Bitcoin, and to deal endogenously with the currency choices of agents. Most importantly, the use of this extended framework allows us to derive a number of new insights, which would not be possible without explicitly modeling the unique technological features.[4]

Both money and Bitcoin are fiat in the model: they have no intrinsic value, as in reality. Both can be used as an MOE in transactions, and agents are allowed to choose either money or 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. First, the government imposes sales taxes on transactions when money is used as an MOE, whereas there is no sales tax on transactions when Bitcoin is used as an MOE. Instead, buyers pay transaction fees to a third party in order to buy goods using Bitcoin. These are so-called *miners* in the Bitcoin system, who validate the ownership of Bitcoin spent, and record its changes in a digital (distributed) ledger.

Second, since Bitcoin exists only in digital form, the existence of agents, such as miners, for the validation and record-keeping of transactions is essential to Bitcoin being used as a means of payment. Importantly, a positive mass of time is required for miners to finish validating and recording transactions, the so-called *mining* in the Bitcoin system. This increases in the number of Bitcoin transactions, on average, because there is a limit to the number of transactions that the Bitcoin system can record within a certain period due to its limited scalability. This time required for the mining work can make sellers reluctant to deliver their goods on the spot, unlike money, because they are exposed to a double-spending risk.

[4]Following the so-called Wallace (1998) Dictum, "Money should not be a primitive in monetary theory,"we do not assume *ad hoc* frictions such as the "cash-in-advance constraint": agents use only a particular currency, money or Bitcoin, in some transactions. Instead, we explicitly model the distinctive technological features of Bitcoin. As pointed out in Nosal and Rocheteau (2011), the cash-in-advance constraint seems particularly odd when currencies have different fundamentals or technological features and, moreover, could eventually lead to misleading results because money functions as a mechanism that reduces the feasible set of allocations in an economy, not as a mechanism that overcomes frictions in transactions.

Specifically, sellers cannot be sure whether the ownership of Bitcoin received in transactions is completely transferred to them, because buyers can use the same Bitcoin, which has been already spent, more than once until the mining is finished completely. If the received Bitcoin turns out to be double spent later, the sellers ownership may never be verified, and thus the Bitcoin cannot be used in the Bitcoin system. Consequently, sellers can be reluctant to deliver their goods immediately. This delayed delivery of goods limits the ability of Bitcoin to facilitate transactions as an MOE.

Third, mining requires effort on the part of miners, which causes a welfare loss because the effort does not produce any consumable goods. On the other hand, the government has to pay for the money operation cost in order to facilitate the role of money as an MOE, that is, printing new currency, transportation, and destruction of mutilated currency. More details about the technical features of Bitcoin that we incorporate into the model are described in Section 1.2.

In this environment, we focus on the equilibrium in which agents are indifferent in terms of their perception of money and Bitcoin as an MOE and, thus, both money and Bitcoin coexist as an MOE. The model suggests a threshold level of the money growth rate in order for both money and Bitcoin to coexist in equilibrium. If the money growth rate is lower than the threshold level, both money and Bitcoin cannot coexist, because the former is strictly more useful (or efficient) than the latter in an exchange. However, this does not mean that an equilibrium where Bitcoin is the only MOE cannot exist. Depending on the agents' expectations in our model, it is always possible that only Bitcoin is used as an MOE, and money is not valued in equilibrium independently of the money growth rate, because both are fiat.[5]

To obtain further implications, we calibrate the model to the U.S. economy, and conduct

[5] In this respect, see Lagos and Wright (2003) and Fernndez-Villaverde and Sanches (2016). Because both central bank-issued money and Bitcoin are intrinsically useless, they are subject to self-fulfilling prophecies, and thus their values can eventually converge to zero owing to changes in agents' expectations irrespective of the economic fundamentals.

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 does an economy where both money and Bitcoin work as an MOE (henceforth, *coexistence economy*). As explained above, when buyers purchase goods in exchange for Bitcoin, the delivery of goods is delayed to avoid double-spending because of the time-consuming mining process. The delayed consumption leads to a utility loss in addition to a loss in welfare caused by the costly mining work itself. This implies that Bitcoin is not as efficient as money as an MOE. Our quantitative analysis shows that the inefficiency of Bitcoin can cause significant welfare losses under the current Bitcoin system. The coexistence of money and Bitcoin generates a welfare loss of 0.048% of consumption, in terms of a consumption-equivalent measure under an inflation rate of 2%.

As the inflation rate increases, the aggregate trade volume and welfare fall in both money-only and coexistence economies because of the increased money holding cost (and thus less real balances). This result is similar to that in a standard money search model, which is the money-only economy. However, agents in the coexistence economy can substitute away money using Bitcoin. Inflation decreases transactions that use money, but increases transactions that use Bitcoin. As a result, the coexistence economy shows a lower decrease in the aggregate quantity of traded goods than that of the money-only economy. Importantly, however, an increase in the aggregate Bitcoin transactions leads to an increase in the average waiting time until a new Bitcoin transaction is validated and recorded in the Bitcoin system, due to its limited scalability. Thus, the delivery of goods purchased using Bitcoin is delayed for a longer time, on average. This delay causes the lower *effective* consumption of buyers, which takes into account a consumption delay. Consequently, welfare falls further in the coexistence economy than in the money-only economy in response to an increase in the inflation rate, and the welfare gap between the two economies widens. Specifically, the welfare loss caused by the coexistence of money and Bitcoin increases from 0.018% to 8.9%

of consumption as the inflation rate rises from zero to 100%.

Finally, we analyze the effects of 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, but 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. The transaction fees decrease the Bitcoin trade volume and thus welfare 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. Notably, however, welfare increases in response to an increase in the transaction fees in the coexistence economy. When both money and Bitcoin are used as an MOE, agents can substitute Bitcoin with money. The aggregate trade volume decreases by less than it does in a Bitcoin-only economy, and the portion of transactions that use a more efficient MOE (i.e., money) increases. Furthermore, the decrease in the Bitcoin trade volume leads to a decline in the average waiting time for confirming Bitcoin transactions, which makes Bitcoin more efficient as an 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 blockchain technology is limited, in spite of its recent rapid growth. Our study can be considered part of the literature on the coexistence and substitutability of central bank-issued money (so-called "outside" money) and privately issued monies ("inside" money) or assets as an MOE; see Kocherlakota (1998), Kocherlakota and Wallace (1998), Cavalcanti and Wallace (1999), Williamson (1999), Berentsen (2006), and Lagos and Rocheteau (2008). Among recent studies, Fernndez-Villaverde and Sanches (2016) build a Lagos and Wright (2005) framework with privately issued currencies in order to study currency competition and its macroeconomic effects. They conclude that a privately issued currency that is not backed by productive capital would be driven out of the economy. Schilling and Uhlig (2018) construct a general equilibrium model with central bank-issued money and Bitcoin. They use the model to study cryptocurrency pricing and to derive the necessary conditions for speculation to occur in equilibrium. Garratt and Wallace (2017) and Athey et al. (2016) investigate the value of Bitcoin and its exchange rate with a sovereign currency. In these studies, however, cryptocurrencies are not considered seriously as a form of privately issued money, or the main technological features of blockchain-based cryptocurrencies such as a mining process for new blocks are not explicitly incorporated within the framework with central bank-issued money.[6] To the best of our knowledge, our work is the first attempt to study how central bank-issued money and a cryptocurrency co-exist and compete within a theoretical framework that includes the distinctive technological features of blockchain-based cryptocurrencies.

Some other recent studies have addressed questions related to the Bitcoin system as a representative cryptocurrency system. For example, Yermack (2013) examines whether Bitcoin is a currency that functions as a medium of exchange, a store of value, and a unit of account, concluding that Bitcoin nearly serves as a speculative asset under the current system. Chiu and Koeppl (2017) study the optimal structure of the Bitcoin system. According to them, the efficiency of the system can be improved by changing its reward mechanism for mining. Specifically, 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, the so-called a network effect, on a blockchain platform on which 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 adop-

[6] Fernndez-Villaverde and Sanches (2016) consider *money-like* features of cryptocurrencies, in the sense that the features are mainly related to their supply process, such as the existence of upper bounds on their supplies and their fixed supply protocols. However, they do not incorporate technological structures of blockchain-based cryptocurrencies.

tion, and thus price variation. Similarly, Gandal and Halaburda (2014) study the network effects on competition between crytopcurrencies and on their relative valuations. However, these studies investigate an economy with a cryptocurrency only, especially Bitcoin. None of these studies examines how a cryptocurrency competes with 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. Chiu and Wong (2015) take a mechanism design approach to discuss how e-money helps to implement constrained efficient allocations. E-money is also a digital currency, but its technical background differs from that of the blockchain-based cryptocurrencies.

In the international macroeconomics and finance literature, Routledge and Zetlin-Jones (2018) show that blockchain distributed ledger technologies can be used to establish currency stability against another currency by removing self-fulfilling speculative attacks on the currency in the model with bank runs of Diamond and Dybvig (1983). In addition, Gandal et al. (2017) and Glaser et al. (2014) focus on cryptocurrency valuations and their volatility against the U.S. dollar as a financial asset, not an MOE.

1.2 A brief introduction to cryptocurrencies

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

Digitalized, or digital, currencies necessarily require trustworthy record-keepers and electronic ledgers, where the current status or changes of ownership are recorded electronically by a series of numbers—a combination of either zeros and ones. The main concern with this feature is that the records can be easily duplicated into other digital memory devices. This 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 digital currencies. The digital currencies, before the recent emergence of cryptocurrencies, eliminated the double-spending risk mainly by authorizing only a few legally qualified financial institutions to record currencies' ownership and keep it on their own digital ledgers.

Cryptocurrencies are also a kind of digital currency that exists only in the form of electronic records on digital ledgers, and are thus exposed to a double-spending risk. Unlike other digital currencies, cryptocurrencies remove this risk by using blockchain technology. A blockchain is a decentralized digital ledger in which anyone can record and keep the complete transaction history, but only if he/she is willing to do so. As a representative example, the Bitcoin system authorizes so-called *miners* to validate and record transactions or changes in its ownership on the blockchain. Being a miner implies being connected through a *node* to the Bitcoin network. A node is a program that validates new transaction records, broadcasts blocks with the records to other nodes, and keeps the chain of blocks.[7] Anyone can become a miner by installing a Bitcoin-mining computer program, which enables the miner to participate in competition for validating and recording Bitcoin transactions, and to maintain changes in Bitcoin ownership through a node.

Specifically, miners compete with one another to be the only one to record new transactions on the blockchain and, thus, earns rewards for it. As a first step, a miner makes or *mines* a new block with collected pending Bitcoin transaction data by determining a cryptographic nonce with which to compute a specific hash value using the hash function dSHA256.[8] The nonces can be found only through a trial-and-error procedure; hence, this process is called proof of work (PoW).[9]

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

[8]See Berentsen and Schar (2018) and Sanches (2018) for technical details on the block creation process and the Bitcoin transaction process.

[9]Among several verification protocols, the Bitcoin system adopts proof of work (PoW) as a verification algorithm, which is the original one used in the first blockchain network. However, there are other algorithms,

Once a miner finds a nonce to yield a specific hash value, the miner broadcasts the mined block to the network as quickly as possible for verification and consensus. If more than half of the total nodes accept it and miners on those nodes use the spread block for the next block creation by attaching it to their own chains of existing blocks, then the miner who made the new block becomes the only winner and receives the rewards.[10] Since the number of nodes that accept the newly created block must be more than 50% of the total in order to win the competition, the blockchain is oftentimes called an "agreed-upon shared distributed database." The current Bitcoin system is programmed to take about 10 minutes, on average, to append a new block to the blockchain, even with advances in computing technology to calculate nonces and hash values.

PoW requires a certain amount of electronic energy and computational usage. The higher computing power (and thus higher investment cost for the computing power) increases the probability that a miner will compute a nonce faster than other miners will, thus winning the competition. Then, the miner earns the corresponding reward of a newly created Bitcoin and transaction fees. The current number of new Bitcoins awarded to a winner is 12.5 Bitcoins.[11] In addition, transaction fees are paid for the mining process. The existence of transaction fees incentivizes miners to first include transactions that pay high fees in the new blocks they create. The current transaction fees remain low, less than 0.001 Bitcoins per transaction, except for a few extreme cases. Bitcoin awarded as a reward for mining may not be spent for the next 100 blocks.[12]

such as proof of stake and proof of capacity. See Ouattara et al. (2018) for technical details on these mechanisms.

[10]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 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.

[11]This reward is halved every 210,000 blocks, and Bitcoin creation is scheduled such that the total number of Bitcoin converges to 21,000,000 units.

[12]Since mining one block currently takes 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 blockchain forks.

Last but not least, a 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 to be recorded in the blockchain when a large number of transactions occur within a period.[13]

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

2 Environment

The basic framework of the model is based on the work of Lagos and Wright (2005), with heterogeneous agents similar to those of Lagos and Rocheteau (2005) 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 number of miners is fixed at η, which is a large positive integer. Agents

[13] Opinion is divided among experts on the scalability of the Bitcoin network, that is, rescaling a block's size. See https://en.bitcoin.it/wiki/Block_size_limit_controversy.' Moreover, scalability problems faced by Bitcoin are discussed by, among others, Croman et al. (2016) and Zheng et al. (2018).

have the following quasi-linear functional forms of preferences in period t, respectively:

$$\text{Buyers: } U(q_t, X_t, H_t) = u(q_t) + X_t - H_t$$

$$\text{Sellers: } U(h_t, X_t, H_t) = -c(h_t) + X_t - H_t$$

$$\text{Miners: } U(e_t, X_t, H_t) = -e_t + X_t - H_t.$$

Here, q_t is consumption in the GM; X_t and H_t are consumption and the labor supply, respectively, in the CM; h_t is the labor supply used to produce goods in the GM; and e_t is the effort (or expenses) for mining in the GM. $u(\cdot)$ is twice continuously differentiable, with the properties of $u'' < 0 < u'$, $u(0) = 0$, $\lim_{q \to 0} u'(q) = \infty$, and $\lim_{q \to \infty} u'(q) = 0$. Moreover, $c(\cdot)$ is twice continuously differentiable, strictly increasing, and strictly convex, with $c(0) = 0$. Each agent can produce one unit of the perishable consumption good for each unit of labor supply in each subperiod, but miners' effort in the GM does not produce any goods.

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. All agents are anonymous; that is, they are unaware of each other's transaction history. Furthermore, they have limited commitment; that is, they are unable to use a credit arrangement. Thus, an MOE is necessary in order for transactions between buyers and sellers to occur in the GM. Two types of currencies can be used as an MOE: money and Bitcoin. Money (M) and Bitcoin (B) are perfectly divisible, storable, and grow at the gross rates 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 $\gamma_b \geq 1$. GM goods can be purchased at the (real) prices of $p_{m,t}$ and $p_{b,t}$, in terms of CM goods in period t, with money and Bitcoin, respectively. Given the prices of GM goods, each buyer chooses demand $q^b_{m,t}$ and $q^b_{b,t}$, purchased with money and Bitcoin, respectively, and each seller chooses supply $q^s_{m,t}$ and $q^s_{b,t}$ in exchange for money and Bitcoin, respectively. Lastly, miners who participate in the mining work expend effort e_t to validate and record transactions where Bitcoin is used as an MOE.

In the second subperiod, the CM opens. All types of agents trade *numeraire* CM goods and currencies—money and Bitcoin—in a 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. The money supply is controlled by the government, which is a consolidated authority. New money is injected into (withdrawn from) sellers through lump-sum transfers (taxes) as standard money search models.[14] On the other hand, there is no authority to control the Bitcoin supply, and the Bitcoin system is programmed to adjust the growth rate, γ_b, according to its predetermined rule.

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

An issue which arises in building up a model is how to incorporate the process to update Bitcoin transaction information on the existing blockchain, preventing the double-spending risk inherent in all cryptocurrencies. We assume that any Bitcoin transactions in the CM are automatically recorded to the existing blockchain without a double-spending risk, due to public monitoring, whereas any Bitcoin transactions in the GM must be verified and recorded by miners. In the verification and recording process, miners competitively create new blocks by expending effort, e_t, in the GM. The probability of winning the competition increases in his/her effort relative to that of other miners. In addition, we assume that the mining games are independent across blocks. That is, miners compete for a new block in each mining game in sequence.

[14] 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, not to sellers. However, the identity of who receives the transfer does not affect the main results.

A miner who succeeds in adding his/her new block to the blockchain is compensated with Bitcoin in the next CM. There are two 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 value of a Bitcoin transaction and fixed at a certain rate of $f > 0$.[15] Second, the miner also receives newly created (or supplied) Bitcoin as a reward for his/her successful mining work. The quantity of the new Bitcoin supplied in the next CM, $\widetilde{S}_t$, is determined by the growth rate, γ_b: $B_t = \gamma_b B_{t-1} = B_{t-1} + \widetilde{S}_t$ (or $\widetilde{S}_t = (\gamma_b - 1)B_{t-1}$). Since the reward cannot be negative, we assume that $\gamma_b \geq 1$, as shown above.

Confirmation lag of Bitcoin transactions and delayed consumption Bitcoin transactions are not 100% secure against the double-spending risk until a transaction record is a certain number of blocks deep. Thus, sellers may not be sure that the Bitcoin paid in transactions completely belongs to them, even if buyers broadcast an electronic message that they have handed over their Bitcoin to the sellers in the Bitcoin network. If a Bitcoin transaction turns out to be a double-spending case later, the sellers' ownership of the received Bitcoin is never verified, and thus the Bitcoin cannot be used 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. This risk and the confirmation lag means that sellers can be reluctant to hand over goods to buyers on the spot. Specifically, we assume that sellers can commit to deliver goods but cannot commit to the timing of delivery in the GM. This implies that if a buyer has incentives of

[15]In reality, buyers can determine 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.

double-spending, then sellers deliver goods only after the Bitcoin transaction is confirmed or 100% secured on the blockchain to avoid double spending. However, in the model, buyers have nothing to lose from double-spending attack, and hence, buyers will commit a double spending attack whenever it is possible.[16] As a consequence, when a buyer purchases goods with Bitcoin, a confirmation lag exists; hence, he/she has to wait before receiving goods.[17]

We reflect this feature in the model by introducing a discount factor, $\delta \in [0,1]$, to the consumption of goods purchased using Bitcoin, $q^b_{b,t}$, similar to iceberg transportation cost models, such as Krugman (1991). This is also in line with that of Chiu and Koeppl (2017).[18] Specifically, the buyer's effective consumption of GM goods in period t, denoted as q^b_t, is given as

$$q^b_t = q^b_{m,t} + \delta q^b_{b,t}.$$

Under the current Bitcoin system, the confirmation lag in a given period t depends on two important factors: the aggregate mining effort, Λ_t, and the aggregate quantity of goods traded using Bitcoin, $q_{b,t}$ in period t. Specifically, we let the discount factor be a function of $\frac{\Lambda_t}{q_{b,t}}$ and $q_{b,t}$, as $\delta\left(\frac{\Lambda_t}{q_{b,t}}, q_{b,t}\right)$, as described below.

First, the discount factor, δ, increases in the aggregate mining effort. This is because the pace of the mining and confirmation process increases in the aggregate mining effort. For example, if there is no mining work, a Bitcoin transaction will never be confirmed, and sellers would not deliver goods for perpetuity. Hence, δ would be zero in this extreme case.

[16] If a buyer has something to lose from double-spending attempts, such as a good reputation of his/her digital wallet, for example, as in Kang (2019), then the buyer may not have double-spending incentives without delivery lags (see Kang (2019) for more information).

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

[18] The way of introducing the discount factor is a bit different from that of Chiu and Koeppl (2017), where only Bitcoin exists as an MOE. They introduce δ in front of the utility function, that is, $\delta u(q)$. However, there are two types of MOE in our model, and the discount factor, δ, should not affect the consumption of goods purchased using money, because buyers receive the goods instantly if money is used. If we introduced δ in front of the utility function, that is, $\delta u(q)$, as in Chiu and Koeppl (2017), it would affect the effective consumption of goods purchased using money as well. To avoid this problem, we introduce δ in front of $q^b_{b,t}$ like iceberg transportation cost models.

Specifically, if n_t number of blocks are created and the aggregate mining effort in period t is Λ_t, then the aggregate mining effort for each block $\frac{\Lambda_t}{n_t}$ affects the time for mining a new block and hence the discount factor. However, the number of blocks increases with the Bitcoin transaction volume.[19] Thus, we assume that the discount factor, δ, is an increasing function of $\frac{\Lambda_t}{q_{b,t}}$, instead of $\frac{\Lambda_t}{n_t}$, and $\delta(0,\cdot) = 0$ for tractability.[20]

Second, the discount factor, δ, decreases in the aggregate quantity of goods traded using Bitcoin, $q_{b,t}$. A new block can contain only a certain number of transaction records, due to its size limit of 1 MB. As the quantity of goods traded using Bitcoin rises in a given period, more blocks need to be created and added to the existing blockchain. This means that a particular Bitcoin transaction may be contained in a later block of the blockchain, delaying the confirmation of the transaction. Thus, as the number of blocks increases the average waiting time before receiving goods increases which implies a decrease in the discount factor δ. Since the number of blocks created depends on the aggregate quantity of goods traded using Bitcoin, $q_{b,t}$, we assume that the discount factor, δ, decreases in the aggregate Bitcoin transaction volume as $\frac{\partial \delta(\cdot, q_{b,t})}{\partial q_{b,t}} < 0$ and $\lim_{q_{b,t} \to \infty} \delta\left(\cdot, q_{b,t}\right) = 0$.

Government expenditure and taxes Government spending in the model comprises government consumption, g_t, and the cost of fiat money operations, g_t^m.[21] Government consump-

[19]An increase in $q_{b,t}$ does not necessarily imply an increase in the number of Bitcoin transactions because a buyer may purchase a large amount of goods from one seller (in a transaction). However, it is also reasonable to assume that an increase in $q_{b,t}$ means more Bitcoin transactions in the following sense. Suppose that each period represents a year. In reality, a buyer would not purchase all goods in one transaction from one seller for consumption of the whole year. He/She will buy and consume goods several times throughout the year. That is, the quantity of goods consumed and the number of transactions are positively correlated. Thus, an increase in the quantity of goods consumed in a given period would mean more transactions in a given period.

[20]Although the aggregate mining effort for each block, $\frac{\Lambda_t}{n_t}$, 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, unless $\frac{\Lambda_t}{n_t}$ remains at too a low level, it does not critically affect the discount factor. We consider this property when calibrating the model in Section 5.

[21]In typical monetary theories, such as Lagos and Wright (2005), government expenditure is not considered explicitly, and lump sum taxes (or transfers) change passively with changes in money growth rate. However, government expenditure plays an important role in an economy, and many quantitative macro models, such as Gertler and Karadi (2011, 2013), explicitly include such expenditure. We allow for government expenditure as in the standard quantitative macro models, but in a stylized way.

tion, g_t, includes any expenditure to produce government services such as national defense and social security. We treat it as exogenous. The cost of the fiat money operations includes printing new currency, transportation, destruction of mutilated currency, verification and removing counterfeit money, and packaging of currency. Various factors, such as the money holding habits of consumers, denomination system of a country, and transaction velocity for each denomination, can affect the money operation cost in reality. Nevertheless, we simply assume that the cost of fiat money operations is proportional to the real value of money transactions in the GM, as $g_t^m = \theta p_{m,t} q_{m,t}$, where $q_{m,t}$ is the aggregate quantity of GM goods traded using money, and 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 studies do. In particular, we include sales tax as a source of government revenue, which is imposed on transactions where money is used as an MOE in the GM 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 the lump-sum taxes. We assume that sellers pay the sales tax, but the identity of who pays this tax does not affect the main results.

Taken together, the government budget constraint is given by

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

Here, $(\gamma - 1)\phi_t M_{t-1}$ is the seigniorage of the money supply, given a 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

In this section, we characterize the optimal behavior of each economic agent. Due to quasi-linearity of preferences, as in Lagos and Wright (2005), the value function for an agent at the beginning of the CM is linear in his/her initial asset holdings. Furthermore, the optimal decisions of agents, such as the choice of asset portfolio for the next GM, are independent of the asset holdings. For example, let $V(m_t, b_t)$ denote the value function for a representative buyer at the beginning of the CM in period t, where the arguments m_t and b_t denote money and Bitcoin balances, respectively. Then, because of the quasi-linearity, we can express the value function as $V(m_t, b_t) = \phi_t m_t + \psi_t b_t + V(0,0)$, which makes the model tractable. Furthermore, we consider the case where $\frac{\phi_t}{\phi_{t+1}} > \beta$ and $\frac{\psi_t}{\psi_{t+1}} > \beta$, because an monetary equilibrium does not exist otherwise. This implies that no agents will carry extra money and Bitcoin into the next CM.

Miners' problem Miners compete to verify Bitcoin transactions in the GM by changing their own effort, e_t. The probability that a miner i will win the mining competition for each block depends on the ratio of his own effort, $e_{i,t}$, to the aggregate effort of all miners to mine a block, $\sum_{j=1}^{\eta} e_{j,t}$. That is, the probability of miner i's winning is given by $\frac{e_{i,t}}{\sum_{j=1}^{\eta} e_{j,t}}$.[22]

By winning the competition for updating the blockchain with a new block in the GM, a miner receives Bitcoin as a reward in the next CM. Specifically, the total rewards for successful mining in period t comprise transaction fees, F_t, and newly created Bitcoin, S_t, both in terms of CM goods. Both F_t and S_t depend on the aggregate quantity of Bitcoin transactions. That is, $F_t = f p_{b,t} q_{b,t}$ and $S_t = r_t p_{b,t} q_{b,t}$, where r_t is the ratio of newly created Bitcoin to the aggregate quantity of Bitcoin transactions. If no transactions use Bitcoin in a given period, that is, $q_{b,t} = 0$, there is nothing to verify and, hence, $F_t = S_t = 0$. The Bitcoin transaction fees are proportional to the total value of the Bitcoin transactions at the fixed rate of f, but

[22] See Chiu and Koeppl (2017) for a micro-foundation for this probability of winning.

r_t is determined by the growth rate of Bitcoin γ_b and B_{t-1}. More precisely, when $q_{b,t} > 0$, $S_t = r_t p_{b,t} q_{b,t} = \psi_t(\gamma_b - 1)B_{t-1}$. Since we focus on equilibria where both money and Bitcoin are traded, that is, $q_{b,t} > 0$, we use the equation, $S_t = \psi_t(\gamma_b - 1)B_{t-1}$, in the following analysis.

In the model, all winners of mining competition share the total reward for mining work, and thus, if $n_t > 0$ number of blocks are mined, then the reward R_t for each successfully mined block is given as

$$R_t = \frac{S_t + F_t}{n_t} = \frac{\psi_t(\gamma_b - 1)B_{t-1} + f p_{b,t} q_{b,t}}{n_t}. \tag{2}$$

Furthermore, the mining games are independent across blocks and miners compete for each block, which implies that miners repeat the same mining game for n_t times and will choose the same strategy for each mining game. A miner i takes the choice of other miners as given and thus the expected profit of a miner i from mining work is given as

$$\pi_{i,t} = \underset{e_{i,t} \geq 0}{Max} \left\{ \psi_t R_t \frac{e_{i,t}}{\sum_{j \neq i} e_{j,t} + e_{i,t}} - e_{i,t} \right\} n_t. \tag{3}$$

where n_t is the number of blocks mined in period t and miners take n_t as given. Substituting (2) into (3), the miner's problem can be re-written as

$$\pi_{i,t} = \underset{e_{i,t} \geq 0}{Max} \left\{ \left[\psi_t(\gamma_b - 1)B_{t-1} + f p_{b,t} q_{b,t} \right] \frac{e_{i,t}}{\sum_{j \neq i} e_{j,t} + e_{i,t}} - n_t e_{i,t} \right\} \tag{4}$$

A miner optimally chooses the effort level, $e_{i,t}$, given other miners' effort. Thus, we obtain

$$\left[\psi_t(\gamma_b - 1)B_{t-1} + f p_{b,t} q_{b,t} \right] \frac{\sum_{j \neq i} e_j}{\left[\sum_{j \neq i} e_{j,t} + e_{i,t} \right]^2} = n_t \tag{5}$$

as the first-order condition, which has a standard interpretation. At the optimum, the expected marginal return from increasing the mining effort for n_t number of blocks on the left-hand side must be equal to its marginal cost of this increase on the right-hand side, which is n_t, given the linear technology for mining work.

Since all miners are homogeneous, we obtain $e_{i,t} = e_t$. Substituting these results into (5), we obtain

$$\left[\psi_t(\gamma_b - 1)B_{t-1} + f p_{b,t} q_{b,t}\right] \frac{\eta - 1}{\eta^2 e_t} = n_t \tag{6}$$

as the Nash equilibrium condition of the mining game. Then, the expected profit from mining work π_t given in (4) and the aggregate mining effort $\Lambda_t = n_t \sum_{j=1}^{\eta} e_{j,t}$ are given as

$$\pi_t = \frac{\left[\psi_t(\gamma_b - 1)B_{t-1} + f p_{b,t} q_{b,t}\right]}{\eta^2} \tag{7}$$

$$\Lambda_t = \left[\psi_t(\gamma_b - 1)B_{t-1} + f p_{b,t} q_{b,t}\right] \frac{\eta - 1}{\eta}. \tag{8}$$

In reality, anyone can become a miner by installing a mining program on his/her computers. Thus, mining work is competitive, and so we let $\eta \to \infty$ to capture this fact.[23] Note, from (7), that as η goes to infinity, the expected profit from mining work π_t converges to zero: competition dissipates the profit from mining work. In addition, the aggregate mining effort Λ_t, given by (8), goes to the aggregate reward for the mining work in a given period. The above analysis is summarized in the next lemma.

Lemma 1 *As $\eta \to \infty$, miner's effort, e_t, for each block and the expected profit from all mining work in the GM, π_t, converge to zero, and the aggregate mining effort Λ_t converges to the aggregate total reward for the mining work in a given period.*

[23] See Buy Bitcoin World (https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there). In addition, according to blockchain.info, there are 14 mining pools that individually can account for at least 1% of the total computation power.

Buyer's problem As explained above, a buyer would not carry 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 in period t:

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

where $q_{b,t+1}$ is the total quantity of GM goods traded with Bitcoin in the GM in period $t+1$. Buyers purchase $q^b_{m,t+1}$ and $q^b_{b,t+1}$ units of GM goods in exchange for money and Bitcoin at the real prices of $p_{m,t+1}$ and $p_{b,t+1}$, respectively. Buyers take as given the aggregate miners' effort, Λ_{t+1}, and the total quantity of GM goods traded using Bitcoin, $q_{b,t+1}$, and, hence, the discount factor $\delta \left(\frac{\Lambda_{t+1}}{q_{b,t+1}}, q_{b,t+1} \right)$. Note that a buyer must pay additional $f p_{b,t+1} q^b_{b,t+1}$ units of real Bitcoin to miners as transaction fees in order to buy GM goods using Bitcoin.

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

$$\frac{\phi_t}{\phi_{t+1}} p_{m,t+1} = \beta u' \left(q^b_{t+1} \right) \tag{9}$$

$$\frac{\psi_t}{\psi_{t+1}} p_{b,t+1}(1+f) = \beta \delta \left(\frac{\Lambda_{t+1}}{q_{b,t+1}}, q_{b,t+1} \right) u' \left(q^b_{t+1} \right), \tag{10}$$

where $q^b_{t+1} = q^b_{m,t+1} + \delta \left(\frac{\Lambda_{t+1}}{q_{b,t+1}}, q_{b,t+1} \right) q^b_{b,t+1}$. The left-hand sides in (9) and (10) can be interpreted as the marginal cost of bringing one additional unit of money and Bitcoin into the GM, whereas the right-hand sides are the present value of the marginal benefit from increasing consumption in the GM using the additional money and Bitcoin, respectively. Note that we can derive an indifference condition between money and Bitcoin from (9) and (10) as follows:

$$\frac{\psi_t}{\psi_{t+1}} \frac{(1+f)}{\delta \left(\frac{\Lambda_{t+1}}{q_{b,t+1}}, q_{b,t+1} \right)} p_{b,t+1} = \frac{\phi_t}{\phi_{t+1}} p_{m,t+1}.$$

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, but no sales tax for 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 that $\frac{\phi_t}{\phi_{t+1}} > \beta$ and $\frac{\psi_t}{\psi_{t+1}} > \beta$. Thus, in the CM, sellers spend all money and Bitcoin, which they earned in the previous GM.[24] The seller's problem in the GM in period t is written as

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

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

$$c'(q^s_{m,t} + q^s_{b,t}) = p_{m,t}(1-\tau_m) \tag{11}$$

$$c'(q^s_{m,t} + q^s_{b,t}) = p_{b,t}. \tag{12}$$

In (11) and (12), the marginal cost of producing GM goods for money and Bitcoin, respectively, must be equal to the marginal benefit from selling them. Here, $p_{m,t}(1-\tau_m)$ represents the real after-tax income from selling one unit of GM goods in exchange for money, and $p_{b,t}$ denotes the real marginal income from selling GM goods in exchange for Bitcoin. Lastly, dividing (11) by (12) yields an indifference condition between money and Bitcoin for sellers as follows:

$$p_{b,t} = p_{m,t}(1-\tau_m). \tag{13}$$

[24] See Rocheteau and Wright (2005) for the precise and careful proof.

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 the 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 $\gamma_b = \frac{\psi_t}{\psi_{t+1}}$. 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 list,* $\left\{z, z_b, q_m^b, q_b^b, q_m^s, q_b^s, q_m, q_b, p_m, p_b, \tau, e, \Lambda\right\}$, *where* $z \equiv \phi_t M_t$ *and* $z_b \equiv \psi_t B_t$, *such that:*

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

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

3. *The mining choice* $\{e\}$ *is a Nash equilibrium of the mining game in the GM;*

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

$$q_m^b = q_m^s \equiv q_m, \tag{14}$$

$$q_b^b = q_b^s \equiv q_b; \tag{15}$$

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

$$z = \gamma p_m q_m, \tag{16}$$

$$z_b = \gamma_b \left[p_b q_b (1+f)\right]; \tag{17}$$

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

To characterize the equilibrium, we substitute the Bitcoin market clearing condition, (17), into (6) to obtain

$$\Lambda = [\gamma_b(1+f)-1]\, p_b q_b, \tag{18}$$

which uniquely determines Λ, given the real value of Bitcoin transactions, $p_b q_b$. In addition, we find the following result because $[\gamma_b(1+f)-1]$ is strictly positive.

Corollary 1 *The aggregate mining effort, Λ, increases in the real value of Bitcoin transactions, $p_b q_b$.*

Next, from (9) − (12), we obtain

$$\frac{\gamma_b(1+f)(1-\tau_m)}{\gamma} = \delta\left(\frac{\Lambda}{q_b}, q_b\right). \tag{19}$$

Because $\delta\left(\frac{\Lambda}{q_b}, q_b\right) \in [0,1]$, the necessary condition for the coexistence equilibrium 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 in equilibrium 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 the Bitcoin growth rate, γ_b, or the transaction fee rate, f, makes Bitcoin less attractive as an MOE. In this case, the inflation rate should increase for coexistence, making buyers and sellers indifferent between Bitcoin and money. Similarly, as the sales tax, τ_m, increases, a lower γ is allowed for both money and Bitcoin 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. This does not mean that Bitcoin cannot be used as an MOE if this necessary condition is violated. As in a standard money search model, an equilibrium in which fiat currency is not valued is always feasible, depending on agents' expectations. Thus, if money is not used as an MOE, and thus $\phi_t = 0$ for all t, then Bitcoin can be used as an MOE with a positive value in equilibrium, even if the condition in Proposition 1 is violated.

Now, we can express q_b and, thus, Λas a function of p_m, using (9), (11), (13), (14), (15), (18), and (19) as follows:

$$(20)\qquad q_b = \widehat{q}_b(p_m) \equiv \frac{\gamma}{\gamma - \gamma_b(1+f)(1-\tau_m)} \left\{ c'^{-1}\left(p_m(1-\tau_m)\right) - u'^{-1}\left(\frac{\gamma p_m}{\beta}\right) \right\}$$

$$(21)\qquad \Lambda = \widehat{\Lambda}(p_m) \equiv (1-\tau_m)\left[\gamma_b(1+f)-1\right] p_m \widehat{q}_b(p_m).$$

Then, substituting (20) and (21) into (19) yields the following equation:

$$(22)\qquad \frac{\gamma_b(1+f)(1-\tau_m)}{\gamma} = \delta\left(\frac{\widehat{\Lambda}(p_m)}{\widehat{q}_b(p_m)}, \widehat{q}_b(p_m)\right).$$

This allows us to obtain the equilibrium value of p_m, given which we can obtain values for p_b, q_m, q_b, Λ, and τ from (1), (11), (12), (16), (20), and (21), which characterizes the whole equilibrium.

Monetary policy and the Bitcoin transaction fee rate We close this section by examining the effects of monetary policy and the Bitcoin transaction fee rate on trading volume by each currency, prices, the aggregate mining effort, and trade surplus in a steady state equilibrium. To provide more intuitive reasoning behind the mechanism through which monetary policy and the transaction fee rate affect the model economy, we make a simplifying assumption for a moment, based on reality. As explained in the introduction, the current Bitcoin system is programmed to take about 10 minutes, on average, to mine a new block. This implies that, unless the aggregate mining effort, Λ, remains at too a low level, its change does not critically affect the waiting time until a Bitcoin transaction is confirmed by mining work, although it could still have minor effects. Based on this reality, we assume for a moment that the aggregate mining effort for each block does not affect the discount factor, δ. Then, δ is a function of q_b only; thus, the equilibrium condition (22) uniquely determines the aggregate quantity of GM goods, q_b, traded using Bitcoin as follows:

$$q_b = \delta^{-1}\left(\frac{\gamma_b(1+f)(1-\tau_m)}{\gamma}\right). \tag{23}$$

We further assume that $[q_b\delta(q_b)]' \geq 0$.

We first study the effects of the monetary policy that determines the inflation rate, γ. Suppose that γ increases. Then, q_b rises by (23). The effects of changing γ on p_m and Λ, which are determined by (20) and (21), respectively, are unclear because the sign of the partial derivative of the right-hand side of (20) with respect to γ is not evident. It depends on the functional form of $c(\cdot)$ and $u(\cdot)$. Next, from (9), we obtain

$$q_m = u'^{-1}\left(\frac{\gamma p_m}{\beta}\right) - q_b\delta(q_b). \tag{24}$$

Thus, if p_m rises when γ increases, q_m falls. On the other hand, if p_m decreases when γ increases, then q_m also falls, according to (11), because q_b increases with respect to γ. Taken together, q_m falls when γ increases; hence, the ratio of the quantity of GM goods traded using 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. Money becomes less attractive to buyers as an MOE, and thus buyers trade more GM goods using Bitcoin and fewer GM goods using money.

	q_m	q_b	p_m	p_b	Λ
γ	$-$	$+$	?	?	?
f	$+$	$-$	$-$	$-$	?

Table 1: Effects of the inflation rate and the transaction fee rate when $\delta = \delta(q_b)$

Next, suppose the Bitcoin transaction fee rate, f, increases. 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 higher transaction fees to purchase GM goods with Bitcoin. A seemingly 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 (20). However, the economic mechanism behind this is as follows. As the transaction fee rate, f, rises, 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, also falls because of the seller's indifference condition (13) for money and Bitcoin. Since both q_b and p_m fall, q_m increases as the transaction fee rate, f, increases, according to (24). Finally, an increase in f has a direct positive effect on the aggregate mining effort, Λ, given in (21), and also the indirect negative effect through p_m and q_b. Thus, it is not evident whether Λ increases or decreases. Table 1 summarizes the above analysis.

How do monetary policy and the Bitcoin transaction fee rate affect the trade surplus, $\mathscr{S}$, which is defined as

$$\mathscr{S} = u\left(q_m + \delta\left(\frac{\Lambda}{q_b}, q_b\right) q_b\right) - c(q_m + q_b) \tag{25}$$

in the GM? In the money search model, the trade surplus is a major part of welfare, which is quantitatively studied in the next section. Thus, an analysis of the trade surplus would provide a better understanding of the mechanism through which monetary policy and transaction fees affect welfare in the model economy. The next proposition describes the effects of monetary policy and transaction fees on the trade surplus.

Proposition 2 *Suppose* $\delta\left(\frac{\Lambda}{q_b}, q_b\right) = \delta(q_b)$. *Then, the trade surplus decreases with* γ *and increases with* f.

Proof. See Appendix. ■

Consider the effects of the inflation rate, γ, first. An increase in γ decreases q_m and raises q_b, as described in Table 1. These two opposite changes affect the total effective consumption, $q_m + \delta(q_b)q_b$, and total production, $q_m + q_b$, and thus the trade surplus. First, an increase in γ raises γp_m, although its effect on p_m is not determined (see the proof of Proposition 2 in the appendix for further details). Thus, $q_m + \delta(q_b)q_b$ decreases in γ by (24). Then, if $q_m + q_b$ (and, thus, the production cost, $c(q_m + q_b)$) increases, then the trade surplus definitely falls. Now, suppose that $q_m + q_b$ decreases in γ, which pushes up welfare by reducing the production cost. Given $\frac{\partial q_m}{\partial \gamma} < 0$ and $\frac{\partial q_b}{\partial \gamma} > 0$, $\frac{\partial [q_m + \delta(q_b)q_b]}{\partial \gamma} < \frac{\partial [q_m + q_b]}{\partial \gamma}$ must hold because $\delta(q_b) \leq 1$. Furthermore, note from (9) and (12) that $u'(q_m + \delta(q_b)q_b) > c'(q_m + q_b)$. Then, the positive effect of increasing γ on the trade surplus by reducing the production cost is dominated by the negative effect of the utility loss from the reduction in effective consumption. Taken together, the trade surplus decreases with the inflation rate γ.

Now, suppose that the transaction fee rate, f, increases, which increases q_m and decreases q_b, p_m, and p_b, as described in Table 1. Given $\frac{\partial p_b}{\partial f} < 0$, total production $q_m + q_b$ must fall by (12). However, effective consumption, $q_m + \delta(q_b)q_b$, increases by (24), given $\frac{\partial p_m}{\partial f} < 0$. This is because a decrease in q_b raises $\delta(q_b)$, making Bitcoin more efficient as an MOE. Thus, the trade surplus increases in γ.

5 Quantitative Analysis

We now turn to a quantitative evaluation of the effects of monetary policy and Bitcoin transaction fees on economic activities and welfare in a steady state equilibrium by calibrating our economy to the United States. We define the sum of expected utilities across agents in a steady state equilibrium as economic welfare. Our welfare measure is given by:

$$W = u\left(q_m + \delta(\frac{\Lambda}{q_b}, q_b)q_b\right) - c(q_m + q_b) - g - \Lambda - \theta p_m q_m. \tag{26}$$

Note that we assume that government expenditure, g, does not increase consumption of agents and thus it is the welfare cost. Alternatively, we can assume that the government provides its services in the form of CM goods which leads to the agents' consumption. However, the main welfare implication does not change. Finally, we subtract aggregate mining effort, Λ, and the cash management cost, $\theta p_m q_m$, as the welfare loss because they do not contribute to the consumption of agents.[25]

5.1 Calibration

The functional forms are standard. The GM utility and cost functions are $u(q) = \frac{(q+\varepsilon)^{1-\alpha} - \varepsilon^{1-\alpha}}{1-\alpha}$ and $c(h) = h^{\sigma}$, where $\varepsilon \approx 0$. The discount factor for Bitcoin transactions is $\delta\left(\frac{\Lambda}{q_b}, q_b\right) = \frac{\Lambda/q_b}{(\delta_1 + \Lambda/q_b)(1+\delta_2 q_b)}$. 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 the curvature of $u(q)$ vary widely in the literature, but we use $\alpha = 1.5$, which is within the range discussed in previous studies. Typical monetary theory literature oftentimes assumes a linear production technology in the GM, but in this case, the Walrasian price, p_b, trivially corresponds to the seller's marginal production cost in the GM. Thus, we use strictly convex

[25] In principle, verification of a Bitcoin transaction can be done by any foreign miners outside of a country. For example, a miner in China can verify a Bitcoin transaction in the U.S. by adding a new block with its information to the blockchain. Specifically, if the proportion of domestic miners to all miners in the world is $\omega \in [0,1]$, then $\omega\Lambda$ is the welfare loss from mining work in the domestic economy. However, foreign miners outside of the country receive the reward for mining work, which is $(1-\omega)\Lambda$ in terms of CM goods given the result of Lemma 1. They will spend the reward in the CM to purchase CM goods, and the labor input to produce $(1-\omega)\Lambda$ units of CM goods for foreign miners does not contribute domestic consumption. Thus, $(1-\omega)\Lambda$ is also welfare cost from mining work. Combined together, the welfare cost from mining work in a steady state equilibrium is Λ.

functions for $c(h)$, and set $\sigma = 2$.[26]

Next, δ_1 influences the effect of aggregate miners' effort for each block on the discount factor $\delta\left(\frac{\Lambda}{q_b}, q_b\right)$. In principle, $\frac{\Lambda}{q_b}$ affects the time to finish the PoW for a new block. However, in reality, the technical structure of Bitcoin was invented such that the average time to mine a new block is 10 minutes. This implies that the miners' effort does not dramatically affect the time taken to mine a new block and, consequently, the discount factor, $\delta\left(\frac{\Lambda}{q_b}, q_b\right)$, although it still has some minor effects. Thus, we set δ_1 sufficiently small, as δ_1 =0.000001. On the other hand, the aggregate quantity of goods traded using Bitcoin has a meaningful effect on the time taken to mine a new block, and thus to confirm a particular transaction. For example, if multiple blocks are mined at almost the same time, each block is added to the blockchain in order, and one transaction 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 described below.

We use the aggregate Bitcoin transaction data, cash management cost, federal government expenditure, monetary base, GDP, and sales tax rates to calibrate the remaining parameters (see Table 2). We use data during the period 2016 to 2017, because certain data, such as the Bitcoin growth rate, transaction volume, and fees before 2016, are unstable due to its intrinsic technical features.[27] We set $f = 0.0007$ to match the ratio of the transaction fees to the Bitcoin transaction value. The average annual growth rate of the Bitcoin stock is 5.7%, that is, $\gamma_b = 1.057$. We calibrate δ_2 to target the ratio of the value of the Bitcoin stock in terms of U.S. dollar to the monetary base in the United States, which is 0.00997 over the period

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

[27]For example, the average growth rate of the Bitcoin supply was approximately 36.16% from 2010 to 2015. The rate decreased approximately from 100% in 2010 to 10% in 2015. In addition, the ratio of the outstanding Bitcoin stock to its approximate limit, 21 million, was just 75% as of July 29, 2015. Source: https://en.bitcoin.it/wiki/Controlled_supply.

from 2016 to 2017.[28] The United States is not the only country that uses Bitcoin, and exact data about the Bitcoin stock circulated within the United States are not available. However, it is well known that "the U.S. has the highest number of Bitcoin users, the highest number of Bitcoin ATMs and also the highest Bitcoin trading volumes globally."[29] We assume that 70% of Bitcoin is used in the United States, and choose $\delta_2 = 8$ to target $\frac{\psi_t B_t}{\phi_t M_t} \approx 0.00997 \times 0.7$. However, the main results do not depend qualitatively on this 70% assumption. We use the average sales tax rate across all states for the period 2016 to 2017 in the United States, and set $\tau_m = 0.065$. The payment system data from the Federal Reserve System indicates that the ratio of cash management costs to GDP for the period 2016 to 2017 in the United States is 0.000065, and we set $\theta = 0.00013$ to target this ratio.[30] Finally, we choose $g = 0.4802$ 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 on economic activities and welfare. Figure 1 shows the steady state values for the macroeconomic variables as a function of the money growth rate, γ, from 1 to 2, that is, from 0% to 100% in terms of the inflation rate. Higher inflation indicates a higher money holding cost, and thus buyers carry less money for transactions. As a result, the quantity of GM goods traded using money decreases as inflation increases, as in the standard monetary

[28] In the calibration of δ_2, we use the following argument. Suppose $\delta_1 = 0$. Then, we obtain $q_b = \frac{1}{\delta_2}\left\{\frac{\gamma}{\gamma_b(1+f)(1-\tau_m)} - 1\right\}$ from (22): q_b decreases with δ_2. Substituting this into (20), we can verify that p_m decreases with δ_2. Thus, according to (24), q_m increases with δ_2. Then, the ratio of the Bitcoin stock to the money stock, which is given as $\frac{\psi_t B_t}{\phi_t M_t} = \frac{\gamma_b(1-\tau_m)(1+f)q_b}{\gamma q_m}$ in a steady state equilibrium, strictly decreases with δ_2. In sum, when $\delta_1 \approx 0$, δ_2 has a monotone negative relationship with the ratio of the Bitcoin stock to the money stock.

[29] In this regard, a number of reports are available online. For example, see 'https://news.bitcoin.com/worlds-top-10-bitcoin-friendly-countries/', and 'https://blogs.thomsonreuters.com/answerson/world-cryptocurrencies-country/'.

[30] 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	"	-	-
δ_1	Coefficient on $\frac{\Lambda}{q_b}$ in $\delta\left(\frac{\Lambda}{q_b}, q_b\right)$	0.000001	"	-	-
f	Bitcoin transaction fee rate	0.0007	Transaction fees/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 $\delta(ME, q_b)$	8	Bitcoin stock/monetary base	0.007	0.007
τ_m	Sales tax rate	0.065	Sales tax rates in the U.S.	0.065	0.065
θ	Marginal cash management cost	0.00013	Cash management cost/GDP	0.00007	0.00007
g	Government expenditure	0.4802	Federal gov. expenditure/GDP	0.2234	0.2235

Table 2: Calibration

theory. Instead, more GM goods are traded using Bitcoin because of the substitution effect caused by the increase in the relative holding cost of money. In particular, the ratio of the quantity of GM goods traded using Bitcoin to the aggregate GM goods production, $\frac{q_b}{q_m+q_b}$, rises from around 0.38% to 21.8%. The increase in Bitcoin transactions leads to an increase in the aggregate transaction fees and, thus, the aggregate mining effort, Λ, increases. The real money price of GM goods, p_m, falls due to a decrease in demand for goods traded using money. This compensates for the increase in the 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 increase in γ has two counteracting effects on government revenue, and thus on the lump-sum tax, τ. On the one hand, since the real value of money transactions, $p_m q_m$, falls, the government net revenue from operating money, $(\tau_m - \theta)p_m q_m$, decreases. On the other hand, as γ rises, the government seigniorage revenue from issuing money increases. The latter effect dominates the former one, and hence the lump-sum tax, τ, falls to balance the government budget.

In the last row of Figure 1, we compare the aggregate trade volume, effective consump-

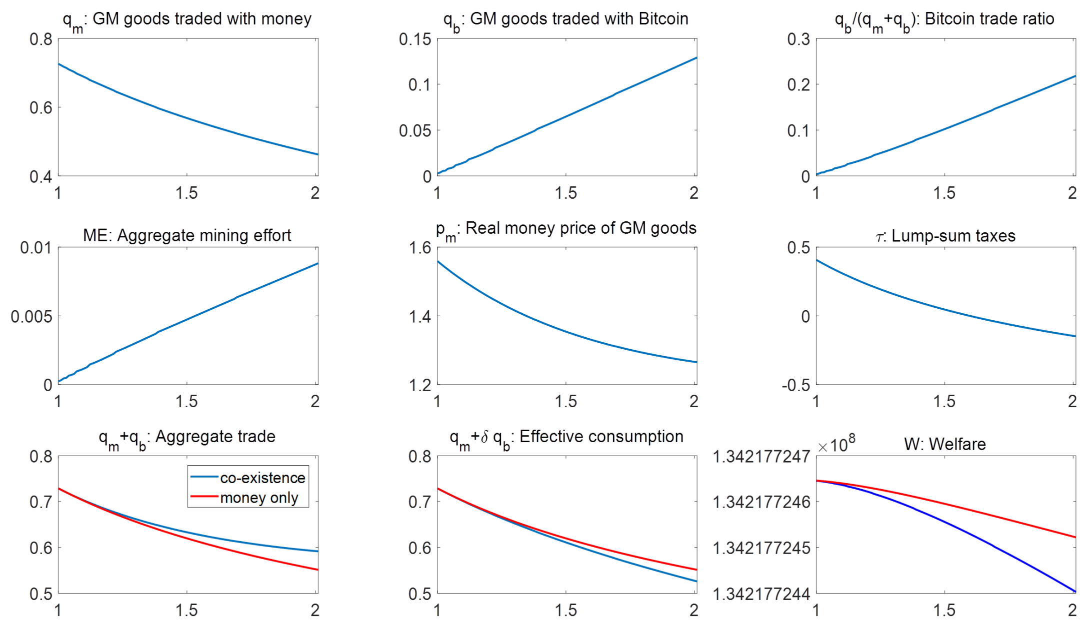

Figure 1: Money growth rate, γ, and aggregate variables

tion, and welfare between an equilibrium where money and Bitcoin coexist (coexistence equilibrium) and an equilibrium where only money is traded as an MOE (money-only equilibrium).[31] As shown in the first graph, when inflation increases, the aggregate trade volume of goods in the GM decreases in both cases, because of the increased money holding cost. However, the total trade volume of goods is higher in the coexistence equilibrium than it is in the money-only equilibrium, and the gap between them expands as the inflation rate increases. This is because buyers in the coexistence equilibrium can choose Bitcoin instead of money as an MOE in transactions, that is, they can pay using Bitcoin for GM goods. Thus, the size of the decrease in the quantity of goods traded in the GM is lower in the coexistence equilibrium than it is in the money-only equilibrium, when inflation rises.

Strikingly, however, overall welfare is lower in the coexistence economy than it is in the money-only economy, as shown in the third graph.[32] The coexistence of money and Bitcoin

[31] 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 Rocheteau and Wright (2005). See Appendix A for the mathematical details about the equilibrium with money only.

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

generates a welfare loss of 0.067% of consumption, in terms of a consumption equivalent measure under an inflation rate of 2%. Moreover, the welfare gap between the two economies expands as inflation increases. Specifically, the welfare loss caused by the coexistence of money and Bitcoin increases from 0.028% to 9.2% of consumption as the inflation rate rises from zero to 100%. The economic mechanism behind this is as follows. The number of Bitcoin transactions that can be contained in a newly created block is restricted by the size limit of each block. As the quantity of goods traded with Bitcoin increases, more blocks need to be created. This implies that it takes longer time on average until a new Bitcoin transaction is validated and recorded in the blockchain; thus buyers have to wait longer time before receiving goods in the GM. This increase in waiting time leads to a decrease in the discount factor $\delta\left(\frac{\Lambda}{q_b}, q_b\right)$ and, consequently, a decrease in the effective consumption, $q_m + \delta\left(\frac{\Lambda}{q_b}, q_b\right) q_b$, and welfare, as shown in the second and third graphs in the last row of Figure 1. Note that each buyer maximizes his/her utility by trading more Bitcoin and less money in the GM in response to an increase in inflation. However, buyers do not internalize the negative externality that an increase in Bitcoin transactions causes greater congestion in the confirmation of Bitcoin transactions in the GM and, thus, a decrease in the discount factor, $\delta\left(\frac{\Lambda}{q_b}, q_b\right)$. In sum, buyers substitute money with Bitcoin, which is less efficient as an MOE. Hence, welfare decreases further in the coexistence economy than it does in the money-only economy as inflation rises.

We now study how an increase in the transaction fee rate, f, affects economic activities and welfare. In a steady-state equilibrium, an increase in f has the same effect as an increase in γ_b, in that f decreases demand for Bitcoin as an MOE by increasing the transaction cost that agents pay for Bitcoin transactions. We focus on the effects of changing f from zero to 0.5. As presented in Proposition 1, if the transaction fee rate is 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 implication does not depend qualitatively on this

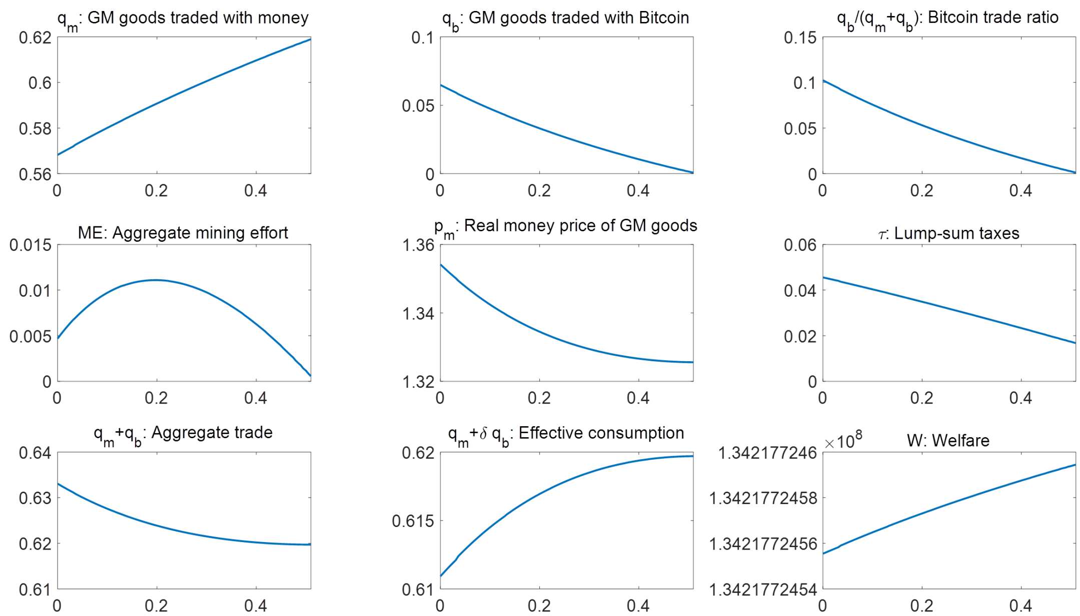

Figure 2: Bitcoin transaction fee, f, and aggregate variables

value of γ. If γ is small, then the upper-bound of f should be sufficiently low; otherwise, there is no meaningful change.

Figure 2 shows the effects of the Bitcoin transaction fee rate on aggregate economic activities and welfare. As the transaction fee rate increases, buyers use more money as an MOE, and thus the quantity of goods purchased using Bitcoin (money) decreases (increases), as shown in the first row of Figure 2. A decrease in demand for Bitcoin pulls down the real Bitcoin price of GM goods, p_b, pushing buyers to use Bitcoin as an MOE in equilibrium. In addition, the equilibrium condition $p_b = p_m(1-\tau_m)$ implies that the real money price, p_m, falls because sellers supply more goods for money. The aggregate mining effort, Λ, exhibits a hump shape, as shown in the second row of Figure 2. When the level of the transaction fee rate, f, is low, an increase in f raises the real value of the aggregate transaction fees, $F = fp_bq_b$, although the real value of the Bitcoin trade volume, p_bq_b, decreases in equilibrium. The higher real value of F increases mining competition, leading to a higher Λ. However, once f is sufficiently high, the real value of F decreases because the negative effect of a decrease in the real value of the Bitcoin trade volume, $p_b q_b$, dominates the positive effect of an increase in f on F. Hence, the aggregate mining effort, Λ, decreases. Next, the effect of an increase in q_m dominates that of a decrease in p_m, and thus the real value of money transactions, $p_m q_m$, increases. This raises government net revenue from operating money, $(\tau_m - \theta) p_m q_m$, and seigniorage by increasing the real value of money stock, $z = \gamma p_m q_m$. As a result, the lump-sum tax τ, which balances the government budget, falls.

The last row of Figure 2 shows the effects of the transaction fee rate on the aggregate trade volume of goods, effective consumption, and welfare. Although an increase in q_m partially substitutes for a decrease in q_b, the aggregate trade volume of GM goods, $q_m + q_b$, decreases as the transaction fee rate, f, increases. However, as each individual agent uses more money, which is a more efficient MOE, to maximize his/her utility, the portion of more efficient transactions in the overall economy increases. Furthermore, as the Bitcoin transactions, q_b, decrease, the average waiting time for the confirmation of a Bitcoin transaction decreases: that is, $\delta\left(\frac{\Lambda}{q_b}, q_b\right)$ increases. This implies that Bitcoin becomes more efficient as an MOE. Consequently, effective consumption, $q_m + \delta\left(\frac{\Lambda}{q_b}, q_b\right) q_b$, increases, and social welfare also increases.

Now, we study the effect of the transaction fee rate, f, in the economy where Bitcoin is the only MOE (or the Bitcoin-only economy), which is similar to other cryptocurrency literature, such as Chiu and Koeppl (2017).[33] This allows us to compare and better understand the effects of the transaction fee rate, f, on economic activities and welfare in the coexistence and Bitcoin-only economies. 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 mining effort increases be-

[33] 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 B for the mathematical details about an equilibrium with only Bitcoin.

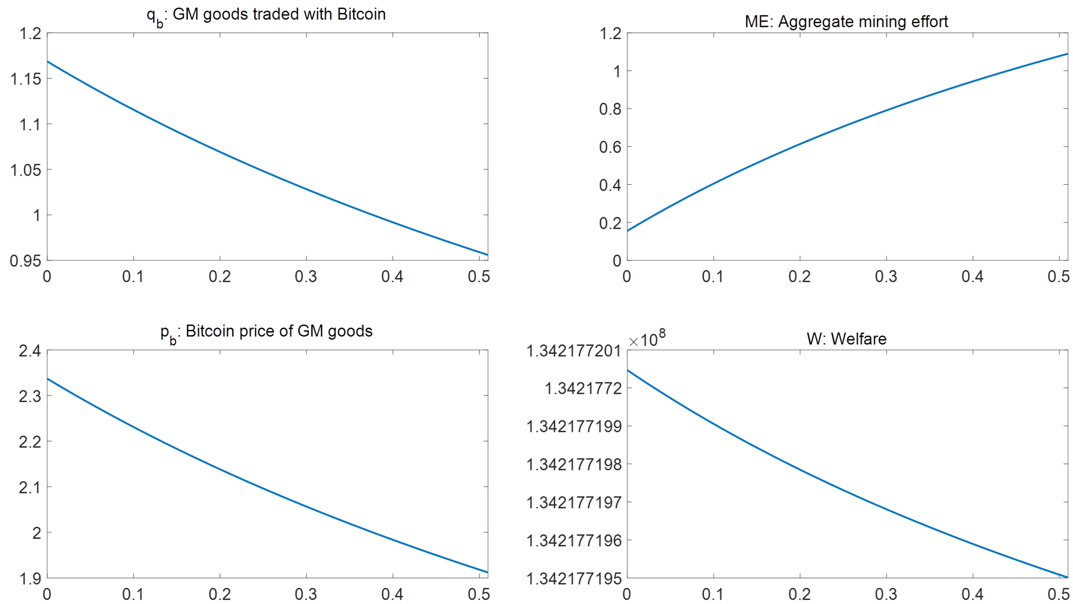

Figure 3: The effects of marginal Bitcoin transaction fee, f, in a economy where Bitcoin is the only medium of exchange

cause f increases the aggregate reward to miners. A key difference from the previous result in the coexistence economy is that welfare decreases as the transaction fee rate increases, which is similar to the policy implication presented in Chiu and Koeppl (2017). This is because the transaction fee rate has the same effect as that of the money holding cost, such as inflation, in a standard money search model, thereby reducing the trade volume in the GM inefficiently. Specifically, although a decrease in q_b and an increase in Λraise $\delta\left(\frac{\Lambda}{q_b}, q_b\right)$, the size of the decrease in q_b is greater than the size of the increase in $\delta\left(\frac{\Lambda}{q_b}, q_b\right)$. Hence, the effective buyer's consumption, $\delta\left(\frac{\Lambda}{q_b}, q_b\right)q_b$, falls. Furthermore, an increase in the costly aggregate mining effort, Λ, has a direct negative effect on welfare. Consequently, the higher transaction fee rate results in lower social welfare.

Last but not least, there exists an economic mechanism through which an increase in the transaction fee rate, f, has the opposite effect on welfare in the coexistence and Bitcoin-only economies. Unlike in the Bitcoin-only economy, buyers in the coexistence economy can substitute Bitcoin with money. This substitution causes two positive effects. First, the aggregate trade volume of goods in the GM decreases by less than it does in the Bitcoin-only economy. Specifically, as the transaction fee rate rises from zero to 0.5, the aggregate trading volume in the Bitcoin-only economy decreases by 18.2%, but the trading volume in the coexistence economy decreases by just 2.1%. In addition, the portion of transactions in which a more efficient MOE is used increases. Unless the cash management cost, θ, is unrealistically high, money is a more efficient MOE than Bitcoin because of the discount factor, $\delta\left(\frac{\Lambda}{q_b}, q_b\right)$. Furthermore, as the quantity of goods traded with Bitcoin, q_b, decreases, the discount factor, $\delta\left(\frac{\Lambda}{q_b}, q_b\right)$, increases. That is, Bitcoin becomes more efficient as an MOE, which implies that even Bitcoin transactions become more efficient as well. Consequently, unlike in the Bitcoin-only economy, an increase in the transaction fee rate improves welfare in the coexistence economy.

6 Conclusion

In this paper, we study whether the central bank-issued money and a cryptocurrency (Bitcoin) compete as an MOE, and how monetary policy and one of the main features of the current Bitcoin system (i.e., transaction fees) affect economic activities and welfare. Our quantitative analysis demonstrates that Bitcoin can compete meaningfully with money only when the inflation rate is sufficiently high, considering the current Bitcoin system. Strikingly, economic welfare in the money-only economy is higher than that in the coexistence economy. The lower welfare in the coexistence economy is primarily attributed to inefficient mining processes and delayed settlements in the current Bitcoin system.

Furthermore, as inflation rises, the welfare gap between the coexistence economy and the money-only economy expands. Specifically, as the inflation rate increases, money is substituted for Bitcoin, which increases Bitcoin transactions. An increase in Bitcoin transactions raises the time for validation and recording Bitcoin transactions due to the restriction on the number of transactions that each block can contain. This, in turn, aggravates the delivery lags of goods when Bitcoin is used as an MOE. Thus effective consumption and welfare decrease further in the coexistence economy.

In addition, welfare increases in the transaction fee rate in the coexistence economy because an increase in the transaction fee rate leads to an increase in money transactions, which is more efficient as an MOE. However, it also leads to fewer Bitcoin transactions, which improves the efficiency of Bitcoin. On the other hand, in the Bitcoin-only economy, economic welfare can be maximized by minimizing the transaction fees which reduce the trade volume of goods.

Lastly, the competition between money and blockchain technology-based cryptocurrencies still requires extensive research, because the technological structure of cryptocurrencies differs from that of existing digitalized currencies, which are built on centralized ledgers. Obviously, current cyptocurrencies are worse than a well-operated central bank money as an MOE. However, as Fernandez-Villaverde (2018) argues that further research will improve the current monetary system. Among others, it would be interesting to examine how a blockchain-based cyrptocurrency in an economy with money should be designed to improve economic welfare, and moreover how the current money system can adapt to technological progress, including blockchain technology. For instance, introducing an alternative mining protocol, such as Proof of Stake, would improve the efficiency of cryptocurrencies as an MOE, and eventually welfare. 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, which would cause significant welfare losses when Bitcoin is widely used as an MOE. This research on cryptocurrencies will help to devise an optimal structure for the Central Bank Digital Currency, which can be newly issued in the near future.[34]

[34]As a representative example, Bordo and Levin (2017) study the optimal design of Central Bank Digital Currency, and also its relevant key features . In addition, recent studies on the Central Bank Digital Currency related macroeconomic issues include Andolfatto (2019), Chiu et al. (2019), and Keister and Sanches (2019).

References

ANDOLFATTO, D. (2019): "Assessing the Impact of Central Bank Digital Currency on Private Banks," Working Papers 2018-25, Federal Reserve Bank of St. Louis.

ATHEY, S., I. PARASHKEVOV, V. SARUKKAI, AND J. XIA (2016): "Bitcoin Pricing, Adoption, and Usage: Theory and Evidence," Research papers, Stanford University, Graduate School of Business.

BERENTSEN, A. (2006): "On the private provision of fiat currency," *European Economic Review*, 50, 1683–1698.

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

BORDO, M. D. AND A. T. LEVIN (2017): "Central Bank Digital Currency and the Future of Monetary Policy," Working Paper 23711, National Bureau of Economic Research.

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., S. DAVOODALHOSSEINI, J. JIANG, AND Y. ZHU (2019): "Central Bank Digital Currency and Banking," Tech. rep., Bank of Canada.

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.

CROMAN, K., C. DECKER, I. EYAL, A. E. GENCER, A. JUELS, A. KOSBA, A. MILLER, P. SAXENA, E. SHI, E. GÜN SIRER, D. SONG, AND R. WATTENHOFER (2016): "On Scaling Decentralized Blockchains," in *Financial Cryptography and Data Security*, ed. by J. Clark, S. Meiklejohn, P. Y. Ryan, D. Wallach, M. Brenner, and K. Rohloff, Berlin, Heidelberg: Springer Berlin Heidelberg, 106–125.

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

FERNANDEZ-VILLAVERDE, J. (2018): "Cryptocurrencies: A Crash Course in Digital Monetary Economics," PIER Working Paper Archive 18-023, Penn Institute for Economic Research, Department of Economics, University of Pennsylvania.

FERNNDEZ-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.

GARRATT, R. AND N. WALLACE (2017): "Bitcoin 1, Bitcoin 2,...: An experiment in privately issued outside monies," University of california at santa barbara, economics working paper series, Department of Economics, UC Santa Barbara.

GERTLER, M. AND P. KARADI (2011): "A model of unconventional monetary policy," *Journal of Monetary Economics*, 58, 17–34.

——— (2013): "QE 1 vs. 2 vs. 3. . . : A Framework for Analyzing Large-Scale Asset Purchases as a Monetary Policy Tool," *International Journal of Central Banking*, 9, 5–53.

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.

KANG, K.-Y. (2019): "Cryptocurrency, Delivery lag, and Double spending history," Working papers, Yonsei University, Department of Finance.

KEISTER, T. AND D. SANCHES (2019): "Should Central Banks Issue Digital Currency?" Tech. rep., Rutgers University and Federal Reserve Bank of Philadelphia.

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.

KRUGMAN, P. (1991): "Increasing Returns and Economic Geography," *Journal of Political Economy*, 99, 483–499.

LAGOS, R. AND G. ROCHETEAU (2005): "Inflation, output, and welfare," *International Economic Review*, 46, 495–522.

——— (2008): "Money and capital as competing media of exchange," *Journal of Economic Theory*, 142, 247 – 258, monetary and Macro Economics.

LAGOS, R., G. ROCHETEAU, AND R. WRIGHT (2017): "Liquidity: A new monetarist perspective," *Journal of Economic Literature*, 55, 371–440.

LAGOS, R. AND R. WRIGHT (2003): "Dynamics, cycles, and sunspot equilibria in 'genuinely dynamic, fundamentally disaggregative' models of money," *Journal of Economic Theory*, 109, 156–171.

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

NOSAL, E. AND G. ROCHETEAU (2011): *Money, payments, and liquidity*, MIT press, Cambridge.

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.

SANCHES, D. R. (2018): "Bitcoin vs. the Buck: Is Currency Competition a Good Thing?" *Economic Insights*, 3, 9–14.

SCHILLING, L. AND H. UHLIG (2018): "Some Simple Bitcoin Economics," Working Paper 24483, National Bureau of Economic Research.

WALLACE, N. (1998): "A dictum for monetary theory," *Quarterly Review*, 20–26.

WILLIAMSON, S. AND R. WRIGHT (2010): "New monetarist economics: Models," in *Handbook of Monetary Economics*, Elsevier, vol. 3, 25–96.

WILLIAMSON, S. D. (1999): "Private Money," *Journal of Money, Credit and Banking*, 31, 469–491.

YERMACK, D. (2013): "Is Bitcoin a Real Currency? An economic appraisal," Working Paper 19747, National Bureau of Economic Research.

ZHENG, Z., S. XIE, H. DAI, X. CHEN, AND H. WANG (2018): "Blockchain challenges and opportunities: a survey," *IJWGS*, 14, 352–375.

Appendix A: Omitted proof

Proof of Proposition 2. We first study the effects of changing the transaction fee rate f on the trade surplus which is given in (25). Suppose that the transaction fee rate f rises. Then, $\delta(q_b)$ rises by (23). In addition, p_m falls, as described in Table 1, which implies an increase in $q_m + \delta(q_b)q_b$ by (24). However, the cost $c(q_m + q_b)$ given by (12) decreases because p_b falls as f rises, as described in Table 1. Thus, the trade surplus increases with the transaction fee rate f.

We now study the effects of the inflation rate γ on the trade surplus. By taking derivative of the trade surplus with respect to γ, we obtain

$$\frac{\partial \mathscr{S}}{\partial \gamma} = u'(q_m + \delta(q_b)q_b)\frac{\partial[q_m + \delta(q_b)q_b]}{\partial \gamma} - c'(q_m + q_b)\frac{\partial[q_m + q_b]}{\partial \gamma}. \tag{27}$$

Note, from (24), that if γp_m increases, $q_m + \delta(q_b)q_b$ decreases. To see the effects of γ on γp_m, we substitute (19) into (20), obtaining

$$q_b[1 - \delta(q_b)] + u'^{-1}\left(\frac{\gamma p_m}{\beta}\right) = c'^{-1}(p_m(1 - \tau_m)). \tag{28}$$

Now, suppose γp_m decreases as γ rises, which requires that p_m must decrease as γ increases. As γ increases, q_b increases, as described in Table 1, which pushes down $\delta(q_b)$ given by (23). Thus, $q_b[1 - \delta(q_b)]$ rises with γ. Furthermore, given the assumption that γp_m decreases as γ rises, the left-hand side of (28) increases as γ increases. However, the right-hand side of (28) increases with p_m, so it decreases with γ, and hence we obtain a contradiction. Thus, γp_m increases as γ rises, and thus, the effective consumption, $q_m + \delta(q_b)q_b$, given by (24), decreases with γ, that is, $\frac{\partial[q_m + \delta(q_b)q_b]}{\partial \gamma} < 0$.

Note that as γ increases, q_m falls and q_b rises (see Table 1). Thus, given $\delta(q_b) \leq 1$, it must be that $\frac{\partial[q_m+\delta(q_b)q_b]}{\partial\gamma} < \frac{\partial[q_m+q_b]}{\partial\gamma}$. Then, substituting (9) and (11) into (27), we obtain

$$\frac{\partial\mathscr{S}}{\partial\gamma} < \left\{\frac{\gamma p_m}{\beta} - p_m(1-\tau_m)\right\}\frac{\partial[q_m+\delta(q_b)q_b]}{\partial\gamma} < 0.$$

Thus, the trade surplus decreases with γ. ■

Appendix B: Money-only economy

In this appendix, we study an economy in which money is the only MOE, which is basically the same as the work of Rocheteau and Wright (2005) with competitive pricing in the decentralized market. In the CM, a buyer solves

$$\underset{q_m^b}{Max}\left\{-\gamma p_m q_m^b + \beta u\left(q_m^b\right)\right\},$$

which gives

$$\gamma p_m = \beta u'\left(q_m^b\right) \tag{29}$$

as the first-order condition.

Next, a seller spends all money and Bitcoin in the CM that she earned in the previous GM. In the GM, the seller's problem is given by

$$\underset{q_m^s}{Max}\left\{-c(q_m^s) + (1-\tau_m)p_m q_m^s\right\},$$

and we obtain

$$c'(q_m^s) = (1-\tau_m)p_m \tag{30}$$

as the first-order condition.

The market clearing conditions are

$$q_m^b = q_m^s = q_m \tag{31}$$

$$z = \gamma p_m q_m, \tag{32}$$

where $z \equiv \phi_t M_t$.

Then, from (29) and (30), we obtain

$$\frac{\gamma c'(q_m)}{1-\tau_m} = \beta u'(q_m), \tag{33}$$

which determines q_m, given γ and τ_m. Then, from (1), (29), and (31) – (33), we obtain the equilibrium market price p_m and the lump-sum tax τ, characterizing the overall equilibrium.

Appendix C: Bitcoin-only economy

In this appendix, we study an economy in which Bitcoin is the only MOE, which implies that there is no money transaction ($q_m = 0$), compared with the coexistence economy. Since there are no variables related to money in the miner's problem, the miner's problem and their optimal choices do not change. However, there are minor changes in other agents' problems because $q_m = 0$ in this economy.

First, a buyer must decide only on how much Bitcoin balances to bring into the GM, and the quantity of GM goods to purchase, q_b^b. Then, in the steady state, the buyer's problem is

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

which yields

$$\gamma_b p_b(1+f) = \beta\delta\left(\frac{\Lambda}{q_b}, q_b\right) u'\left(\delta\left(\frac{\Lambda}{q_b}, q_b\right) q_b^b\right) \tag{34}$$

as the first-order condition.

Next, since the government imposes a sales tax only on money transactions in the GM, a seller in the Bitcoin-only economy does not pay sales tax. In addition, the seller decides the supply of GM goods, q_b^s, in exchange for Bitcoin. Thus, the seller's problem is

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

which gives us

$$c'(q_b^s) = p_b \tag{35}$$

as the first-order condition.

The market clearing conditions are

$$q_b^b = q_b^s = q_b, \tag{36}$$

$$z_b = \gamma_b p_b q_b(1+f), \tag{37}$$

where $z_b = \psi_t B_t$.

Then, from (5), (18), and (35) − (37), we can express Λas a function of q_b, which is given by,

$$\Lambda = \widehat{\Lambda}_b(q_b) = [\gamma_b(1+f)-1]c'(q_b)q_b. \tag{38}$$

Then, substituting (35) − (37), and (38) into (34), we obtain

$$\gamma_b c'(q_b)(1+f) = \beta\delta\left(\frac{\widehat{\Lambda}_b(q_b)}{q_b}, q_b\right) u'\left(\delta\left(\frac{\widehat{\Lambda}_b(q_b)}{q_b}, q_b\right) q_b\right),$$

which gives the equilibrium value of q_b. Then, we can obtain the values for p_b and $\Lambda$from (35) and (38), and $\tau = g$ by (1).