On the Coexistence of Cryptocurrency and Fiat Money

Zhixiu Yu*

October 2021

Abstract

This paper studies the conditions under which cryptocurrency is valued and under which it coexists with fiat money, using search-theoretic models. A cryptocurrency economy is one in which private agents determine the stock of money and in which the marginal cost of producing money depends on the existing stock in circulation. I show that the inflation rate must be zero in a stationary monetary equilibrium. This result is in sharp contrast to models with fiat money in which the stock of money is exogenously given. In fiat money economies, the inflation rate is determined by the rate of growth of the money stock. My result is also in sharp contrast with other types of private money economies, in which the inflation rate must necessarily be different from zero. In such private money economies, the cost of producing additional money does not depend on the existing stock. I show that cryptocurrency and fiat money can circulate at the same time and that the rates of return on these two assets may not be the same. Gresham's Law does not hold in the sense that, even if cryptocurrency is costly to produce and less acceptable, cryptocurrency can coexist with fiat money, a widely accepted asset that is costless to produce.

JEL Classification: E40, E50

Keywords: Cryptocurrency, Private Money, Currency Competition, Money Search

*University of Minnesota, Department of Economics, 4-101 Hanson Hall, 1925 Fourth Street South, Minneapolis, MN, 55455, United States. E-mail: yuxx0616@umn.edu. First draft: January 2021. Recent version of the paper can be obtained at `https://www.zhixiuyu.com`. I am very grateful to V.V. Chari for his guidance and support throughout this project. I thank Gabriele Camera, Micheal Choi, Lucas Herrenbrueck, Larry Jones, Qingxiao Li, Fernando Martin, Christopher Phelan, Guillaume Rocheteau, Agustin Samano, Dan Su, Neil Wallace, Christopher Waller, Randall Wright, Ariel Zetlin-Jones, Lichen Zhang, and Yu Zhu for their helpful comments and suggestions, as well as participants from the Public Workshop at the University of Minnesota, the 2019 Midwest Economics Association at St. Louis, the 2019 Summer Workshop on Money, Banking, Payment and Finance at the Bank of Canada, and the Macro Brownbag Seminar at the University of California Irvine.

1. Introduction

The emergence of Bitcoin has triggered a large wave of public interest in cryptocurrencies. Unlike most common forms of fiat currency such as dollars or euros, cryptocurrencies are not backed by a central bank or any government authorities. As predetermined by a computer algorithm, the new cryptocurrency is produced by computer servers ("miners") who are willing to solve complicated computational problems using programming efforts. The predetermined program algorithm makes cryptocurrencies costly to produce, and the number of new cryptocurrencies that can be produced is decreasing in the total money stock. This deflationary property of cryptocurrency may preclude the over-issuance problem, which happens to fiat money when government tends to raise its seigniorage by over-issuing money (see, e.g., Araujo and Camargo (2006, 2008)).

There has been growing interest in cryptocurrencies, and this growing interest raises several questions: Under which conditions can this currency be valued in equilibrium? Can it provide price stability? Under which conditions can it coexist with government-issued fiat money? Would this privately-issued currency be welfare-enhancing? The goal of this paper is to provide a theoretical framework to address these issues.

To that end, I first develop a search-theoretic model of an economy with a privately-produced money—cryptocurrency. My framework builds on the workhorse model of monetary exchange by Lagos and Wright (2005), in which agents interact periodically in a decentralized market characterized by bilateral random matching, where there is a need for liquid assets, and also interact periodically in a centralized market, where agents can adjust their asset portfolios. I adapt the Lagos-Wright (LW) environment by adding a new type of private agents—profit-maximizing miners—who are the sole issuers of cryptocurrency. The LW framework is particularly insightful for addressing currency issues because the acceptability of a medium of exchange is determined endogenously in equilibrium, and the LW framework is amenable to analysis and allows me to incorporate a miner sector while keeping the distribution of currency holdings analytically tractable.[1]

My model highlights two key attributes of cryptocurrency: it is private money, and it is costly to produce. Its supply is endogenous and driven by the production decisions of miners, who have access to a costly mining technology that recognizes the legitimacy of cryptocurrency. The production cost is not only increasing in the amount of newly produced units, but also increasing in the aggregate stock of cryptocurrency that has been produced and is still in circulation. This is a key feature that makes cryptocurrency different from other types of private money in the

[1] Kiyotaki and Wright (1989, 1993) are the first-generation search-theoretic models that incorporate a double-coincidence problem with indivisible money and output to show the essentiality of a medium of exchange. Shi (1995) and Trejos and Wright (1995) relax the assumption of indivisible goods and endogenize prices. The assumption of indivisible money is relaxed in Lagos and Wright (2005). Surveys and summaries of the literature which study currency issues in the search-theoretical environment are provided by Williamson and Wright (2010), Nosal and Rocheteau (2011), and Lagos et al. (2017).

literature, in which the production cost function is independent of the existing stock of money, e.g., Fernández-Villaverde and Sanches (2019). These assumptions are intended to capture the deflationary property of cryptocurrency. For example, when producing Bitcoin, there are costs associated with the production such as computer power and electricity, and the new Bitcoin mining rewards halve every 210,000 blocks.[2] Thus, the cost of mining the same amount of Bitcoin gets more expensive as more Bitcoin is minted. Conceptually, cryptocurrency does look like gold in the way that the marginal cost of minting gold goes up as miners mine more gold, given that the total amount of gold on the earth is limited. The assumption on the production cost function emphasizes the difference between cryptocurrency and other types of private money, e.g., bank notes, since it is not clear whether the production cost of those private monies depends on their outstanding stock. In this paper, my analysis applies not only to cryptocurrencies such as Bitcoin, but more broadly to any intrinsically worthless object that is privately produced and costly to produce, which may serve as a medium of exchange.[3]

Moreover, I model the cryptocurrency law of motion by assuming that the stock of cryptocurrency in each period is determined by both the newly produced units and the depreciation from the last period. The amount of new cryptocurrency is endogenously determined by miners, while the depreciation is modeled to capture the loss of cryptocurrency. In particular, I assume that a proportion of the cryptocurrency holdings from the last period will be lost in each period. These assumptions are intended to capture the idea that cryptocurrency is more vulnerable to being lost because people sent it to a wrong address, or lost or discarded their device, or forgot their password which has complicated strings, etc.[4] Unlike most types of medium of exchange, such as cash or commodity money, which can be reused after getting lost, once a cryptocurrency is lost, it might be lost forever, and other people can not reuse it.[5]

In the economy with cryptocurrency only, I show that given that the marginal production cost depends on the existing stock of money, the inflation rate must be zero in a stationary monetary equilibrium. That is, the price and the stock of cryptocurrency must remain constant, and all the

[2]Bitcoin block is used to store the bitcoin transaction information. Miners who successfully mine a new block are rewarded through a number of new bitcoin. The bitcoin reward is halved every 210,000 blocks, which takes around four years to complete. See more on: `https://www.investopedia.com/terms/b/block-reward.asp`.

[3]There has been literature on other cryptocurrency issues related to the double-spending problems, competitive mining process, or transaction fees (e.g., Iwasaki (2020) and Chiu and Koeppl (2019)), and on its role as a speculative asset (e.g., Zhou (2020)). Since in my model, cryptocurrency is produced according to a technology that allows its recognizability as legitimate, issues related to double spending, recognizability, or counterfeiting are not relevant in the context of the model environment.

[4]According to Chainalysis, a blockchain analysis company, about 23% of the bitcoin currently in circulation may be lost forever. See `https://medium.com/luno-money/where-do-lost-bitcoins-go-7e8dd24abd0f` for more information on the issue of cryptocurrency loss.

[5]The lost cryptocurrency can not be reused since the lost passwords cannot be restored and the transactions cannot be reversed. The stolen bitcoin does not count as loss/depreciation because the thieves have access to it. For literature on identity theft and currency security, see, e.g., He et al. (2005), Kahn and Roberds (2008), and Kahn et al. (2020).

newly produced units only replace the depreciation in equilibrium. It is necessary to have currency depreciation in order for a stationary monetary equilibrium to exist, in which miners constantly produce new money. My result is in sharp contrast to models with fiat money in which the stock of money is exogenously given, e.g., Lagos and Wright (2003, 2005). In fiat money economies, the inflation rate is determined by the rate of growth of the money stock, and it can be different from zero as long as the stock of money changes over time. My result is also in sharp contrast with other types of private money economies, in which the cost of producing additional money is independent of the existing stock. In such private money economies, as Fernández-Villaverde and Sanches (2018) claim, a monetary equilibrium will not deliver price stability because profit-maximizing producers always have an incentive to create an additional unit of money. Their conjecture does not hold in my cryptocurrency economy, in which the marginal production cost increases in the existing stock. In this economy, there is no incentive for miners to produce cryptocurrency in excess of the flow of currency exogenously lost, and thus, the price of cryptocurrency can remain constant in equilibrium. To make this argument explicit, I show that if I make the marginal production cost independent of the aggregate stock in my model and set the currency depreciation rate to zero, then a monetary equilibrium necessarily has positive inflation, which implies that the claim in Fernández-Villaverde and Sanches (2018) is correct in a version of my model with different assumptions about technology.

Next, to explore the coexistence of cryptocurrency and fiat money, I extend my cryptocurrency-only model by adding government-issued fiat money and multiple decentralized markets into the economy. Fiat money differs from cryptocurrency in the issuers, supply rules, production costs, and degrees of acceptability in decentralized markets (probabilities that agents visit the markets in which sellers accept that currency as a payment method). Fiat money is exogenously supplied and is costless to produce. It is issued by the government according to a deterministic growth rule. Changes in fiat money supply are injected or withdrawn in a lump-sum fashion to agents. There are three decentralized markets: DM1, DM2, and DM3, which differ in the currencies that can be accepted as payment methods. Specifically, agents can only trade with fiat money in DM1, e.g., transactions that accept cash only or involve the government authorities; agents can only trade with cryptocurrency in DM2, e.g., online Bitcoin stores or black markets where fiat money is not used; and agents can trade with both currencies in DM3, e.g., AT&T, PayPal, Microsoft, etc.[6] In each period, agents randomly enter one of the decentralized markets with a certain probability. The market structure of my two-currency model is analogous to that of the two-currency, two-country search models for studying international currencies and exchange rates, e.g., Zhang (2014) and Zhu and Wallace (2020).[7] The assumption of currencies with different degrees of acceptability in

[6]See more on `https://bitpay.com/directory` and `https://99bitcoins.com/bitcoin/who-accepts/`.

[7]The earliest two-country, two-currency search-theoretic environment was proposed by Matsuyama et al. (1993). Zhou (1997) develops it by allowing for currency exchange. There are many papers in the search literature that look at multiple-currency issues with the invisibility assumption on currencies. However, they are not suitable to analyze

markets is akin to the cash-in-advance assumptions in Lucas (1982), which constrain agents to use one type of currency in a particular trade.

Similar to what happens in multiple-fiat currency models, e.g., Camera et al. (2004) and Engineer (2000), there are currency regimes with neither, both, or only one of the currencies that are valued in the economy of cryptocurrency and fiat money, depending on the fundamentals and parameters of the model. Though the probability that agents visit each decentralized market is exogenous, the acceptability of a currency is endogenous in the following sense. There exists an equilibrium in which there are no markets where fiat money is used for transactions, including DM1; there exists an equilibrium in which there are no markets where cryptocurrency is used, including DM2; and there exists an equilibrium in which both currencies are circulating. However, different from traditional two-fiat currency models, where rates of return on two currencies cannot be different if both currencies are in circulation, e.g., Kareken and Wallace (1981), cryptocurrency and fiat money can coexist regardless of their rates of return in my model. Since each currency is essential in some decentralized meetings, agents will choose to hold both currencies in order to smooth their consumption in all decentralized markets, so long as neither currency is too costly to carry. Thus, a low-return currency can coexist with a high-return currency.

Moreover, my model of cryptocurrency and fiat money has a novel difference, compared to other models of currency competition with payment acceptability constraints, such as a model of fiat monies, e.g., Zhang (2014), and a model of private and fiat monies, e.g., Zhu and Hendry (2019). In their models, the cost of carrying one currency is tied with the exogenous growth rate of the money supply; while in my model, the cost of carrying cryptocurrency depends not only on the exogenous parameters, such as currency depreciation, but also on the endogenous production decisions of miners, which rely on the production cost function and further affect the price path of cryptocurrency in equilibrium. Due to the shape of the cost function of producing cryptocurrency, a monetary equilibrium with coexistence is consistent with a zero inflation rate in cryptocurrency.

Further, since agents can trade with both cryptocurrency and fiat money in some decentralized meetings, the real values of the two currencies are interdependent. When one currency becomes more costly to use or less useful in decentralized markets, agents would demand less for that currency and instead substitute the other currency for transactions. Then the real value of that currency decreases, whereas the real value of the other one increases. In particular, cryptocurrency becomes more costly to carry if it is lost at a higher rate or its marginal production cost diminishes, whereas fiat money becomes more costly to use if it is issued at a higher growth rate. In addition, a currency becomes more useful when its acceptability degree gets larger. As the inflation rate of cryptocurrency is zero in a stationary monetary equilibrium, the competition with cryptocurrency restricts the government's ability to over-issue fiat money for raising its seigniorage.

monetary growth and inflation. See Craig and Waller (2000) for a survey of search literature on multiple currencies.

I then analyze the coexistence of the two currencies under special cases in terms of their degrees of acceptability in markets. In the first case, the decentralized markets are entirely segmented, i.e., the probability of both currencies being accepted by a seller is zero. In this set-up, there is a dichotomy between two currencies' sectors. That is, changes in the fundamentals of one currency through the cost of carrying it would not affect the other currency. In the second case, I assume that one currency has an inherent advantage, modeled as degrees of acceptability in decentralized markets, relative to the other currency. For example, cryptocurrency has an inherent advantage if it is always accepted while fiat money is only partially accepted in markets. In this set-up, agents will carry the currency that can be used everywhere in order to facilitate trades in decentralized markets, so the rate of return on the less acceptable currency must be sufficiently high, in order to give agents enough incentive to carry it as well. Further, Gresham's Law —"Bad money drives out good money"— does not hold in this economy, because both "bad" and "good" assets can circulate in equilibrium. Cryptocurrency, which is, in some sense, inferior in production costs and degrees of acceptability in decentralized markets, can coexist with fiat money, an asset that is more acceptable and costless to produce, when appropriate monetary policy is implemented. This is different from previous work on commodity monies, e.g., Velde et al. (1999), and on fiat monies, e.g., Camera et al. (2004). The former paper shows that Gresham's Law holds in an economy with heavy and light coins, in the way that bad money is always traded while good money is traded if and only if the seller is informed. In contrast, the latter paper characterizes good and bad money by purchasing power risk and shows that agents favor spending the safe money and holding on to the risky one for subsequent trades, where Gresham's Law has been reversed.[8]

The way that cryptocurrency can affect the circulation of fiat currency raises the question: should the government ban cryptocurrency? It depends on the acceptability degree of cryptocurrency and whether the government can commit to maintaining the targeted fiat money growth rule. Since cryptocurrency is costly to produce, banning cryptocurrency can avoid the resource waste on production. But it may worsen the total welfare because agents can only trade using fiat money in decentralized meetings and, thus, there is no trade surplus in DM2, where only cryptocurrency is accepted. In addition, the competition with cryptocurrency restricts the government's ability to over-issue fiat money. The policy implication of my analysis is that if the acceptability degree of cryptocurrency is small and the government can maintain sufficiently low inflation, then banning cryptocurrency would be welfare-enhancing. There would be welfare gains from avoiding resource

[8]Curtis and Waller (2000) also show that the good money—a domestic currency—and the bad money—a foreign currency that is illegal to use in internal trade transactions—can circulate simultaneously despite legal restrictions. They demonstrate that the values of two indivisible currencies are interdependent, and public policy may worsen the value of the domestic currency. In my paper, I explore other properties of currencies, such as growth rates, production costs, and degrees of acceptability in decentralized meetings. With the indivisibility assumption on currencies relaxed, my model is able to analyze the effects of monetary policy on currency usage.

waste on producing cryptocurrency and from consuming more DM goods using fiat money, which outweigh the welfare loss from no trade surplus in DM2. Otherwise, if the government tends to overissue fiat money, then banning cryptocurrency would worsen the total welfare because there would be large welfare loss from consuming fewer outputs using fiat money in markets and no trade surplus in DM2. As cryptocurrency is consistent with zero inflation in a stationary monetary equilibrium, the government that tends to use the inflation tax has a strong incentive to ban the use of cryptocurrency.

My paper is related to two branches of a large literature on multiple currencies that are competing as media of exchange. One branch is the literature where no currency is privately produced. The other branch, where my paper belongs, is the literature where at least one of those currencies is privately produced. For instance, Kareken and Wallace (1981) show that, without portfolio restriction, two exogenously supplied fiat currencies are perfect substitutes, and the rates of return on two currencies must be the same for both currencies in circulation. Lagos and Rocheteau (2008) also show that fiat money and capital can coexist only if they have the same rate of return. My results are different from theirs. I show that fiat money and cryptocurrency can coexist and that the rates of return on these two assets may not be the same. This is driven by the assumption that the two currencies have different degrees of acceptability in decentralized markets. Thus, each currency is essential in some transactions.[9]

There is a growing literature on cryptocurrency issues. For instance, Schilling and Uhlig (2019) analyze the price dynamics of bitcoin. They show that bitcoin prices form a martingale and the risk-adjusted real return on bitcoin and the dollar has to be identical when both currencies are simultaneously in use. You and Rogoff (2019) study the competition between online retailer-issued tokens and bank debit accounts, and focus on issuers' sale and issuance strategies. My emphasis is different from theirs. I focus on the coexistence of cryptocurrency and fiat money in a stationary equilibrium, and I show that the two currencies can coexist with different rates of return. In addition, my paper has it in common with Choi and Rocheteau (2020b) and Zhu and Hendry (2019) that two competing currencies have different degrees of acceptability in decentralized meetings. However, one of the central points my paper focuses on is that if cryptocurrency is costly to produce and the aggregate new cryptocurrency is endogenously determined by miners, what sorts of equilibria are possible? In contrast, the aggregate mining rate of cryptocurrency is exogenously determined in Choi and Rocheteau (2020b), and the private money is costless to produce in Zhu and Hendry (2019). Thus, these papers cannot have an analog of the monetary equilibrium in which the price of cryptocurrency must be constant.

My paper is also related to an extensive literature on currency competition where the issuers of private money are costly operating sectors, e.g., banks. He et al. (2008) and Chari and Phelan

[9]Hu and Rocheteau (2013) provide a summary of approaches that explain different rates of return across assets.

(2014) develop an economy where fiat money and bank deposits serve as means of payment. In the former paper, cash is low-cost but subject to theft, while bank deposit are in safekeeping, but the bank is costly to operate. They show that with exogenous theft, there is no concurrent circulation of both currencies. In the latter paper, bank deposits serve a socially useful insurance role and are privately useful because the bank pays interest on deposits, but banks are costly and subject to bank runs. The authors show that there is no equilibrium in which fiat money and bank deposits coexist. My results are different from those in their papers. Cryptocurrency and fiat money can coexist in equilibrium, even if cryptocurrency is costly to produce. Moreover, unlike those papers with fractional reserve banking, there is no reserve requirement in my model, and the cryptocurrency that is produced by miners is not associated with any promise to exchange for goods or assets in the future.

The rest of this paper proceeds as follows. Section 2 lays out a monetary environment of an economy with cryptocurrency only. Section 3 studies the equilibrium of the cryptocurrency-only model. Section 4 presents an environment with cryptocurrency and fiat money in the economy. Section 5 characterizes the equilibrium of the two-currency model. Section 6 explores the coexistence of two currencies under some special cases. Section 7 concludes.

2. A Model of Cryptocurrency Only

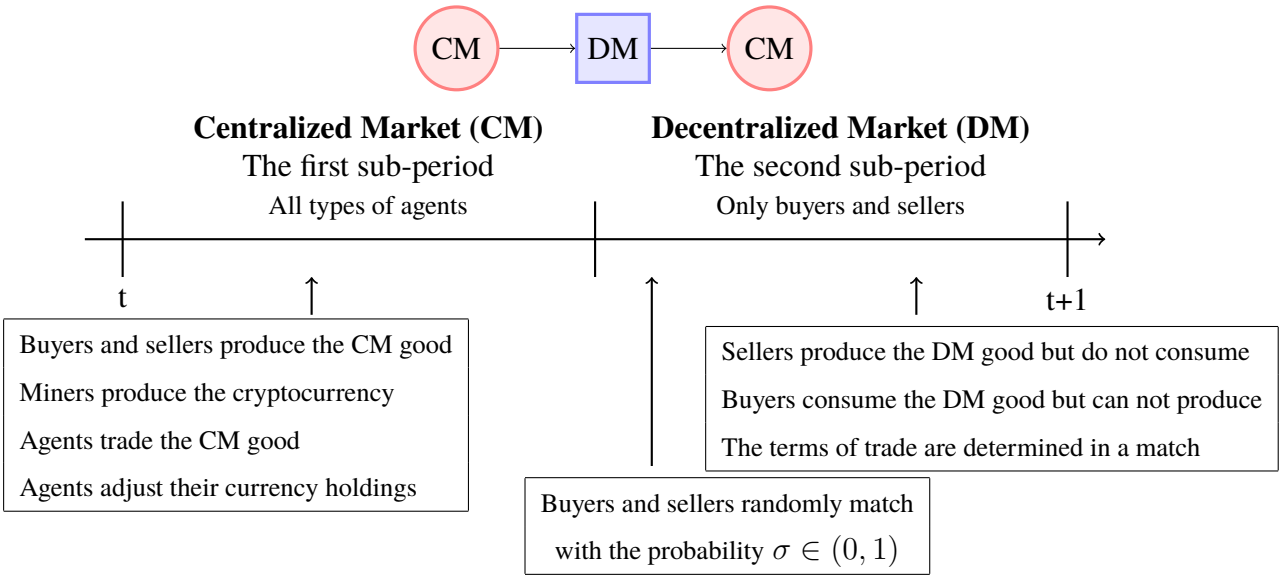
There are three types of infinitely lived agents in the economy: *buyers, sellers*, and *miners*. Each of them are populated with a [0,1]-continuum, and agents' types are permanent. Time is discrete and continues forever. Agents discount the future between periods with a discount factor $\beta \in (0, 1)$, and β is common across all agents. Each period is divided into two sub-periods, in which different economic activities take place. Figure 1 summarizes the timing of events in a typical period.

In the first sub-period, all agents interact in a frictionless centralized market (CM). Agents want to consume a numéraire good, called the CM good, but only buyers and sellers are able to produce it using a linear production function in labor, i.e., one unit of labor produces one unit of the CM good. Miners produce cryptocurrency according to a costly technology that allows its recognizability as legitimate, and immediately sell the newly produced units. All agents adjust their cryptocurrency holdings by producing or consuming the CM good, and the utility from the CM good is linear in consumption and production for all agents. Specifically, one unit of consumption generates one unit of utility, while one unit of production generates one unit of disutility.

In the second sub-period, miners remain idle. Sellers and buyers meet pairwise and at random in a decentralized market (DM). In particular, a buyer is randomly matched with a seller with the

probability $\sigma \in (0,1)$ and vice versa.[10] The consumption good that is produced and traded in the decentralized market is called the DM good. Sellers can produce the DM good using a divisible technology that requires effort as an input, but they do not want to consume; buyers want to consume the DM good but cannot produce. Miners neither consume nor produce the DM good. Since buyers and sellers anonymously meet in the decentralized market, their trading histories are private information and credit cannot be used. Thus, a medium of exchange is essential for trading, see, e.g., Kocherlakota (1998) and Wallace (2001). In each match, the terms of trade are determined by a take-it-or-leave-it offer by a buyer. Specifically, the buyer offers the seller a trade of d_t units of cryptocurrency for q_t units of the DM good, and the seller can accept or reject the buyer's offer.

Figure 1: **Timing of Events in a Typical Period**



All consumption goods are non-storable and perfectly divisible. The perishability of CM and DM goods prevents them from being used as means of payment. Let $x_t \in \mathbb{R}$ denote an agent's net consumption of the CM good, and $q_t \in \mathbb{R}_+$ denote an agent's consumption of the DM good. The preferences of a typical buyer, seller, and miner are represented by the following quasi-linear instantaneous utility functions:

$$U^b(x_t^b, q_t) = x_t^b + u(q_t)$$
$$U^s(x_t^s, q_t) = x_t^s - \omega(q_t)$$
$$U^i(x_t^i) = x_t^i$$

[10] Camera (2000) models two matching technologies that agents can choose from: costless bilateral matching technology, which matches traders according to a random process, and costly multilateral matching technology, which allows deterministic matches but incurs utility costs.

where b, s, i refer to a typical buyer, seller, and miner, respectively. The function $u(q_t) : \mathbb{R}_+ \to \mathbb{R}$ denotes the utility function of a buyer to consume q_t units of the DM good, and $\omega(q_t) : \mathbb{R}_+ \to \mathbb{R}_+$ denotes the cost function of a seller to produce q_t units of the DM good. The functions $u(q_t)$ and $\omega(q_t)$ satisfy the following assumption.

Assumption 2.1. *The functions $u(\cdot)$ and $\omega(\cdot)$ are twice continuously differentiable, such that $u'(q_t) > 0$, $u''(q_t) < 0$, $\omega'(q_t) > 0$, $\omega''(q_t) \geq 0$, and satisfy $u(0) = 0$, $u'(0) = \infty$, $\omega(0) = 0$, $\omega'(0) = 0$, $\omega''(0) = 0$.*

2.1. ***Cryptocurrency***

A medium of exchange is supplied only in the form of cryptocurrency. Its supply is endogenous and driven by the production decisions of profit-maximizing miners. Let M_t denote the aggregate stock of cryptocurrency in period t. Each period, a typical miner i produces δ_t^i units of new cryptocurrency with the cost $c(\delta_t^i, M_{t-1})$. A key feature of cryptocurrency is that its production cost is not only increasing in the newly produced units, δ_t^i; it also strictly increases in the aggregate cryptocurrency stock that is in circulation, M_{t-1}. The production cost function satisfies the following assumption.

Assumption 2.2. *The cost function of producing cryptocurrency, $c(\delta_t^i, M_{t-1}) : \mathbb{R}^2 \to \mathbb{R}$, is increasing, convex, and twice differentiable, i.e., $\frac{\partial c(\delta_t^i, M_{t-1})}{\partial \delta_t^i} > 0$, $\frac{\partial^2 c(\delta_t^i, M_{t-1})}{\partial \delta_t^{i2}} > 0$, $\frac{\partial c(\delta_t^i, M_{t-1})}{\partial M_{t-1}} > 0$, and has positive cross derivatives, i.e., $\frac{\partial^2 c(\delta_t^i, M_{t-1})}{\partial M_{t-1} \partial \delta_t^i} > 0$, $\frac{\partial^2 c(\delta_t^i, M_{t-1})}{\partial \delta_t^i \partial M_{t-1}} > 0$.*

The net circulation of cryptocurrency in each period is determined by both the newly produced cryptocurrency and the depreciation, such that:

$$M_t = M_{t-1} + \Delta_t - \kappa M_{t-1}, \quad \Delta_t \geq 0, \quad M_{-1} \text{ given.} \tag{1}$$

The aggregate new cryptocurrency, Δ_t, is endogenously determined by miners' productions, and the currency depreciation, κM_{t-1}, captures the lost cryptocurrency, which can not be reused by other people.[11] I assume that in each period, a proportion $\kappa \in (0, 1)$ of the cryptocurrency stock from the last period will be lost.[12]

[11] In Appendix B, I alternatively model the cryptocurrency security as theft instead of loss. In that case, thieves have access to the stolen cryptocurrency. I show that there is a unique stationary monetary equilibrium, and in that equilibrium, no cryptocurrency is produced.

[12] Unlike modeling the currency depreciation as loss, Qiao and Wallace (2020) model the currency physical depreciation as worn currency and study the ways of financing the costly replacement of depreciated currency.

Cryptocurrency is perfectly divisible, recognizable, and non-counterfeitable. It is also intrinsically worthless and is not associated with any promise to exchange for goods in the future.[13] Agents are able to predict miners' production behaviors by solving their maximization problems. Thus, agents can form beliefs about the exchange value of cryptocurrency in current and future periods. Let $p_t \in \mathbb{R}_+$ denote the value of cryptocurrency per unit in terms of the CM good in period t.

2.2. *Buyers and sellers*

First, I describe the problems of buyers and sellers in the cryptocurrency economy. They interact in both the centralized and decentralized markets in each period.

2.2.1. *The Centralized Market Problems*

In the first sub-period, a typical buyer b and seller s enter the centralized market with m_{t-1}^b and m_{t-1}^s units of cryptocurrency from the last period, respectively. Due to the idiosyncratic trading shocks in the decentralized market, agents begin a period with different cryptocurrency holdings. In the centralized market, a certain fraction, κ, of the cryptocurrency holdings that an agent brings to the market is lost. A typical buyer and seller choose their net consumption of the CM good, x_t^b and x_t^s, and cryptocurrency holdings to bring forward to the decentralized market, m_t^b and m_t^s, respectively.

Let $W_t^j(m_{t-1}^j)$ denote the value function of an agent beginning a period in the centralized market with $m_{t-1}^j \in \mathbb{R}_+$ units of cryptocurrency from the last period, and $V_t^j(m_t^j)$ denote the value function of an agent entering the decentralized market with $m_t^j \in \mathbb{R}_+$ units of cryptocurrency that are chosen to carry forward, $j \in \{b, s\}$. Then the maximization problems of a buyer and seller in the centralized market are represented by:

$$W_t^j(m_{t-1}^j) = \max_{x_t^j, m_t^j} \quad x_t^j + V_t^j(m_t^j), \quad s.t. \quad x_t^j + p_t m_t^j = p_t(1-\kappa)m_{t-1}^j, \quad j \in \{b, s\} \tag{2}$$

The above CM value functions can be rearranged as:

$$W_t^j(m_{t-1}^j) = p_t(1-\kappa)m_{t-1}^j + \underbrace{\max_{m_t^j \in \mathbb{R}_+} -p_t m_t^j + V_t^j(m_t^j)}_{W_t^j(0)}, \quad j \in \{b, s\} \tag{3}$$

[13] Different from cryptocurrency, there is value in use for commodity monies, such as gold and silver. For example, the jewelry is made of gold.

From (3), an agent j's choice of cryptocurrency holdings at t is independent of the initial cryptocurrency holdings when entering the centralized market, and the cryptocurrency loss, $j \in \{b, s\}$. Thus, there is no wealth effect on the agent's choice of cryptocurrency holdings. All buyers choose the same units of cryptocurrency, m_t^b, and all sellers choose the same units of cryptocurrency, m_t^s.[14]

Lemma 2.1. *Under the quasi-linear preferences, the distribution of cryptocurrency holdings is degenerate to all agents of a given type at the beginning of each second sub-period.*

The optimal cryptocurrency holdings can be obtained by taking the first-order conditions (F.O.C.) of (3) with respect to m_t^j, such that

$$-p_t + V_t^{j'}(m_t^j) \leq 0 \qquad \text{“}=\text{”} \text{ if } \; m_t^j > 0, \quad j \in \{b, s\} \tag{4}$$

where $V_t^{j'}(m_t^j)$ is determined by the decentralized market problem of agent $j \in \{b, s\}$.

2.2.2. ***The Decentralized Market Problems***

In the second sub-period, buyers and sellers enter the decentralized market with their chosen cryptocurrency holdings, m_t^b and m_t^s, respectively. The DM value functions for a buyer and seller are represented by:

$$V_t^b(m_t^b) = \max_{q_t, d_t} \; \sigma[u(q_t) + \beta W_{t+1}^b(m_t^b - d_t)] + (1-\sigma)\beta W_{t+1}^b(m_t^b) \tag{5}$$

$$V_t^s(m_t^s) = \sigma[-\omega(q_t) + \beta W_{t+1}^s(m_t^s + d_t)] + (1-\sigma)\beta W_{t+1}^s(m_t^s) \tag{6}$$

where (q_t, d_t) are the terms of trade.

In the decentralized market, a buyer randomly matches with a seller with the probability $\sigma \in (0, 1)$ and vice versa. In each match, the buyer makes a take-it-or-leave-it offer to the seller over the terms of trade. If the seller accepts it, then the buyer consumes q_t units of the DM good with utilities $u(q_t)$ and transfers d_t units of cryptocurrency to the seller. In the next period, the cryptocurrency holdings that the buyer brings to the centralized market will be reduced to $m_t^b - d_t$. In contrast, the seller produces q_t units of the DM good with costs $\omega(q_t)$ and receives d_t units of

[14]The CM value function (3) remains the same if I alternatively assume that with the probability κ, agents lose all the cryptocurrency holdings from the last period. Specifically, with the probability κ, an agent solves: $\max_{x_t^j, m_t^j} \; x_t^j + V_t^j(m_t^j) \; s.t. \; x_t^j + p_t m_t^j = 0$, which is simplified to: $\max_{m_t^j} \; -p_t m_t^j + V_t^j(m_t^j) = W_t^j(0)$. With the probability $1-\kappa$, an agent solves: $\max_{x_t^j, m_t^j} \; x_t^j + V_t^j(m_t^j) \; s.t. \; x_t^j + p_t m_t^j = p_t m_{t-1}^j$, which is simplified to: $p_t m_{t-1}^j + \max_{m_t^j} -p_t m_t^j + V_t^j(m_t^j) = p_t m_{t-1}^j + W_t^j(0)$. Then the CM value function can be expressed as: $\kappa W_t^j(0) + (1-\kappa)[p_t m_{t-1}^j + W_t^j(0)] = (1-\kappa) p_t m_{t-1}^j + W_t^j(0), j \in \{b, s\}$.

cryptocurrency from the buyer. Thus, in the next period, the seller will carry $m_t^s + d_t$ units of cryptocurrency forward to the centralized market. Otherwise, with the probability $1 - \sigma$, a buyer and a seller are not matched. Then the buyer and seller proceed to the next period with the same cryptocurrency holdings that they bring into the decentralized market, $m_t^j, j \in \{b, s\}$.

In each match, the buyer's take-it-or-leave-it offer to the seller is given by the solution to:

$$\begin{aligned} \max_{q_t, d_t} \quad & u(q_t) + \beta W_{t+1}^b(m_t^b - d_t) \\ s.t. \quad & -\omega(q_t) + \beta W_{t+1}^s(m_t^s + d_t) \geq \beta W_{t+1}^s(m_t^s) \\ & d_t \leq m_t^b \end{aligned} \tag{7}$$

where the first constraint is the seller's participation constraint and the second one is the buyer's liquidity constraint. According to (3), problem (7) can be simplified as follows.

$$\begin{aligned} \max_{q_t, d_t} \quad & u(q_t) - \beta p_{t+1}(1-\kappa) d_t \\ s.t. \quad & -\omega(q_t) + \beta p_{t+1}(1-\kappa) d_t \geq 0 \\ & d_t \leq m_t^b \end{aligned} \tag{8}$$

Under Assumption 2.1, there exists a level of the traded amount of the DM good $q^* > 0$, $q^* = \text{argmax } [u(q_t) - \omega(q_t)]$, that a buyer and a seller would agree on in each decentralized match. If a buyer brings more than what he/she needs to get q^*, then only the first constraint binds and the buyer would pay for q^*, i.e., $q_t = q^*, d_t = m_t^* = \frac{\omega(q^*)}{\beta p_{t+1}(1-\kappa)}$. Otherwise, if a buyer cannot afford q^*, then both of the two constraints bind and the buyer would spend all the cryptocurrency holdings to purchase the DM good, i.e., $d_t = m_t^b, q_t = \hat{q}_t = \omega^{-1}(\beta p_{t+1}(1-\kappa) m_t^b)$ and $\hat{q}_t < q^*$. The solutions to problem (8) are summarized in the following Lemma.

Lemma 2.2. *The terms of trade (q_t, d_t) that solve problem (8) are given by:*

$$q_t(m_t^b) = \begin{cases} q^* & if \quad m_t^b \geq m_t^* \\ \hat{q}_t & if \quad m_t^b < m_t^* \end{cases} \qquad d_t(m_t^b) = \begin{cases} m_t^* & if \quad m_t^b \geq m_t^* \\ m_t^b & if \quad m_t^b < m_t^* \end{cases} \tag{9}$$

where $q^* = argmax\ [u(q_t) - \omega(q_t)]$, $\hat{q}_t = \omega^{-1}(\beta p_{t+1}(1-\kappa) m_t^b)$, and $m_t^* = \frac{\omega(q^*)}{\beta p_{t+1}(1-\kappa)}$.

Lemma 2.3. *Following Lemma 2.2, $\hat{q}_t'(m_t^b) > 0$ and $\hat{q}_t < q^*, \ \forall m_t^b < m_t^*$.*

2.2.3. ***The Optimal Cryptocurrency Holdings***

Following Lemmas 2.1 and 2.2, the optimal cryptocurrency holdings of a buyer and seller are given by the solutions to:

$$W_t^b(m_{t-1}^b) = \max_{m_t^b \in \mathbb{R}_+} -(p_t - p_{t+1}\beta(1-\kappa))m_t^b + v_t(m_t^b) \tag{10}$$

$$W_t^s(m_{t-1}^s) = \max_{m_t^s \in \mathbb{R}_+} -(p_t - p_{t+1}\beta(1-\kappa))m_t^s + 0 \tag{11}$$

$$\text{where } v_t(m_t^b) = \begin{cases} \sigma[u(q^*) - \omega(q^*)] & if \quad m_t^b \geq m_t^* \\ \sigma[u(\hat{q}_t(m_t^b)) - \omega(\hat{q}_t(m_t^b))] & if \quad m_t^b < m_t^* \end{cases}$$

The first terms on the right-hand side (RHS) of (10)-(11) represent the cost of carrying money to the next period, while the second terms represent the expected surplus of an agent in the decentralized market. From (10)-(11), cryptocurrency is costly to carry when $\frac{p_t}{p_{t+1}} > \beta(1-\kappa)$. Since buyers are the ones to make a take-it-or-leave-it offer in a match, buyers have all the bargaining power and take all the gains, whereas sellers have no surplus from trades in the decentralized market.[15]

Intuitively, in the centralized market, a buyer and seller choose the optimal cryptocurrency holdings to maximize their expected surplus from using them in the decentralized market net of the costs of carrying them. Because sellers have no surplus in the decentralized market, there is no strict incentive for them to carry cryptocurrency out of the centralized market.

The optimal cryptocurrency holdings for a buyer and seller can be obtained by taking the F.O.C. of (10)-(11) with respect to m_t^b and m_t^s, respectively.[16]

Lemma 2.4. *The optimal cryptocurrency holdings of a typical buyer and seller must satisfy:*

$$\frac{p_t}{\beta p_{t+1}(1-\kappa)} - 1 \geq \sigma L(m_t^b) \qquad \text{“} = \text{”} \ \textit{if} \quad m_t^b > 0 \tag{12}$$

$$\textit{where } L(m_t^b) = \begin{cases} 0 & \textit{if} \quad m_t^b \geq m_t^* \\ \{\frac{u'(\hat{q}_t(m_t^b))}{\omega'(\hat{q}_t(m_t^b))} - 1\} > 0 & \textit{if} \quad m_t^b < m_t^* \end{cases}$$

$$-p_t + \beta p_{t+1}(1-\kappa) \leq 0 \qquad \text{“} = \text{”} \ \textit{if} \quad m_t^s > 0 \tag{13}$$

The term $L(m_t^b)$ is a liquidity factor that captures the marginal payoff that a buyer can get from using cryptocurrency to purchase more DM outputs in the decentralized meeting instead of carrying it to the next centralized market. That is, $L = 0$ when a buyer can afford q^*, whereas $L > 0$ when a buyer can not afford it.

[15] For the search literature on alternative trading protocols that determine the terms of trade in decentralized meetings, see, e.g., Li (2011) that considers the generalized Nash Bargaining, and Aruoba et al. (2007) that study the Nash and egalitarian solutions.

[16] Equivalently, the optimal cryptocurrency holdings for a buyer and seller can be derived using (4). The resulting conditions will be same as (12)-(13), with $V_t^{b'}(m_t^b) = \beta p_{t+1}(1-\kappa) + v_t'(m_t^b)$ and $V_t^{s'}(m_t^s) = \beta p_{t+1}(1-\kappa)$.

Lemma 2.4 states that if an agent chooses to hold a cryptocurrency, the marginal cost of carrying it must equal the marginal benefit of using it in the decentralized market. According to (12)-(13), when $\frac{p_t}{p_{t+1}} < \beta(1-\kappa)$, there would be infinite demand on cryptocurrency because its return is too high, and therefore, the market would not clear. When cryptocurrency is costless to carry, i.e., $\frac{p_t}{p_{t+1}} = \beta(1-\kappa)$, buyers would carry enough cryptocurrency to obtain q^*. In that case, there is no value for agents to carry an additional unit of cryptocurrency to the decentralized market. In contrast, when cryptocurrency is costly to carry, i.e., $\frac{p_t}{p_{t+1}} > \beta(1-\kappa)$, sellers would not hold cryptocurrency, and buyers would only carry what they expect to spend in the decentralized meeting. In a match, buyers would spend all the cryptocurrency holdings, m_t^b, to purchase the DM good, $\hat{q}_t < q^*$, and they value an additional unit of cryptocurrency that they carry to the decentralized market.

Lemma 2.5. *Under Assumption 2.1, the DM value function of a buyer b, $V_t^b(m_t^b)$, is concave $\forall m_t^b < m_t^*$, and the buyer's cryptocurrency holdings, m_t^b, can be uniquely determined by:*

$$\frac{p_t}{p_{t+1}} - \beta(1-\kappa) = \beta\sigma(1-\kappa)[\frac{u^{'} \circ \omega^{-1}(\beta p_{t+1}(1-\kappa)m_t^b)}{\omega^{'} \circ \omega^{-1}(\beta p_{t+1}(1-\kappa)m_t^b)} - 1] \tag{14}$$

*2.3. **Miners***

Next, I describe the problem of miners. Miners only participate in the centralized market during the first sub-period and remain idle during the second sub-period.

In the centralized market, a typical miner i chooses the consumption of the CM good, x_t^i, and the amount of new cryptocurrency to produce, δ_t^i. There are costs associated with the currency production, $c(\delta_t^i, M_{t-1})$, which depend on the newly produced units and the existing cryptocurrency stock.[17] Miners sell all newly produced cryptocurrencies at price p_t right after production.[18] The maximization problem of a typical miner is represented by:

$$\begin{aligned} \max_{x_t^i, \delta_t^i} \quad & \sum_{t=0}^{\infty} \beta^t x_t^i \\ \text{s.t.} \quad & x_t^i \leq p_t \delta_t^i - c(\delta_t^i, M_{t-1}) \quad \forall t \\ & x_t^i, \delta_t^i \geq 0 \qquad \forall t \end{aligned} \tag{15}$$

[17] In this paper, I model the production cost of cryptocurrency as a resource cost. All the results would be the same if the production cost is modeled as a utility cost. In addition, unlike modeling the cost function and technology in my economy, Choi and Rocheteau (2020a) assume that miners produce private monies according to a time-consuming technology and they face opportunity costs due to occupation choice.

[18] Since miners remain idle in the second sub-period, they do not have an incentive to carry cryptocurrency out of the centralized market. Appendix E.1 relaxes this assumption and shows that, even if miners are allowed to carry cryptocurrency, they will still choose to sell all the newly produced units after the production in equilibrium.

Given (15), the miner's problem in period t can be written as follows.

$$\max_{\delta_t^i \geq 0} \quad p_t \delta_t^i - c(\delta_t^i, M_{t-1}) \tag{16}$$

Lemma 2.6. *Under Assumption 2.2, a typical miner i produces δ_t^i units of cryptocurrency in period t, given p_t and M_{t-1}, such that:*

$$\delta_t^i = \max[0, f(p_t, M_{t-1})] \tag{17}$$

where $f(p_t, M_{t-1})$ results from the F.O.C. of (16): $p_t = \frac{\partial c(\delta_t^i, M_{t-1})}{\partial \delta_t^i}$, which is expressed as $\delta_t^i = f(p_t, M_{t-1})$.

Example 2.1. *Suppose the cost function of producing cryptocurrency is taken the functional form: $c(\delta_t, M_{t-1}) = DM_{t-1}\delta_t + B\delta_t^2,\ B, D > 0$, which satisfies Assumption 2.2. In this case, a miner i would produce $\delta_t^i = \max[0, \frac{p_t - DM_{t-1}}{2B}]$ units of cryptocurrency in period t.*[19]

From (17), the number of new cryptocurrency in each period depends on the value and the stock of cryptocurrency. Further, the aggregate new cryptocurrency in period t, Δ_t, becomes:

$$\Delta_t = \int_0^1 \delta_t^i di = \max[0, f(p_t, M_{t-1})] \tag{18}$$

Given the above conditions, we can formally define an equilibrium.

3. Equilibrium

Definition 1. *An equilibrium is a set of decision rules in the centralized market $\{x_t^b, m_t^b, x_t^s, m_t^s, x_t^i, \delta_t^i\}_{t=0}^{\infty}$, the terms of trade $\{q_t, d_t\}_{t=0}^{\infty}$, and sequences of value and aggregate stock of cryptocurrency $\{p_t, M_t\}_{t=0}^{\infty}$, such that for all $t \geq 0$,*

1. *$x_t^b, m_t^b, x_t^s, m_t^s$ solve problems (2) and (5)-(6) for buyers and sellers;*
2. *q_t, d_t solve problem (7) and satisfy (9);*
3. *x_t^i, δ_t^i solve problem (15) for miners;*
4. *the cryptocurrency law of motion is satisfied:*

$$M_t = (1 - \kappa)M_{t-1} + \Delta_t, \quad \textit{where} \quad \Delta_t \textit{ satisfies (18);}$$

[19] Appendix F describes the equilibrium outcomes of the cryptocurrency-only economy with the production cost function specified in Example 2.1.

5. *the cryptocurrency market clear:*
$M_t = M_t^b + M_t^s$, *where* $M_t^b = \int_0^1 m_t^b db$, $M_t^s = \int_0^1 m_t^s ds$;
6. *the centralized good market clear:*
$\int_0^1 x_t^b db + \int_0^1 x_t^s ds + \int_0^1 x_t^i di + \int_0^1 c(\delta_t^i, M_{t-1}) di = 0$.
7. *the transversality condition is satisfied:*
$\lim_{t\to\infty} \beta^t p_t M_t = 0$.

Definition 2. *A monetary equilibrium is an equilibrium in which the price of cryptocurrency is strictly greater than zero.*

Definition 3. *A stationary equilibrium is an equilibrium in which the real balance of cryptocurrency is constant over time, i.e.,* $p_t M_t = p_{t+1} M_{t+1} = z^{ss}$.

3.1. Stationary Equilibrium

This section characterizes the stationary equilibrium in the economy with cryptocurrency only. Since cryptocurrency has no intrinsic value, there is always a non-monetary stationary equilibrium s.t. $p_t = p_{t+1} = 0$, and therefore, $z^{ss} = 0\ \forall t$. In what follows, I focus on the stationary equilibrium in which cryptocurrency is valued and produced.[20]

I first investigate whether there exists a monetary equilibrium in which the price of cryptocurrency is constant. Next, I examine the equilibrium in which the price changes at a constant rate.

Proposition 1. *Under Assumptions 2.1 and 2.2, there exists a unique stationary monetary equilibrium in which the price of cryptocurrency is constant. The equilibrium outcomes are characterized by:*

$$\frac{1-\beta(1-\kappa)}{\sigma\beta(1-\kappa)} = [\frac{u' \circ \omega^{-1}(\beta z^{ss}(1-\kappa))}{\omega' \circ \omega^{-1}(\beta z^{ss}(1-\kappa))} - 1] \tag{19}$$

$$f(p^{ss}, M^{ss}) = \kappa M^{ss} \tag{20}$$

$$1 + \frac{1-\beta(1-\kappa)}{\sigma\beta(1-\kappa)} = \frac{u'(q^{ss})}{\omega'(q^{ss})} \tag{21}$$

$$\Delta^{ss} = \kappa M^{ss} \tag{22}$$

[20] Appendix A.2 presents a stationary monetary equilibrium in which no cryptocurrency is produced.

Proposition 2. *Under Assumptions 2.1 and 2.2, there is no stationary monetary equilibrium in which the price of cryptocurrency changes at a constant rate.*

Propositions 1 and 2 present the main results of the cryptocurrency economy: given that the marginal cost of producing cryptocurrency strictly increases in the existing stock of money, there exists a stationary equilibrium in which cryptocurrency is valued, and the inflation rate must be zero in a stationary monetary equilibrium. In that equilibrium, the stock of cryptocurrency remains constant, and all the newly produced cryptocurrencies only replace the currency depreciation in every period. That is, if there is no cryptocurrency loss, then no cryptocurrency is produced in equilibrium. It is necessary to have currency loss/depreciation in order for a stationary monetary equilibrium to exist, in which miners constantly produce new money. For many types of cryptocurrency, such as Bitcoin, miners secure the trading system through mining new coins. Moreover, as Proposition 1 shows, the equilibrium quantity traded in the decentralized market is less than the socially efficient quantity, $q^{ss} < q^*$. The stationary monetary equilibrium with a stable price of cryptocurrency is not socially efficient.

Why must the price of cryptocurrency be constant in a stationary monetary equilibrium? In the cryptocurrency economy, the money supply is endogenously determined by the production decisions of miners, and the cost of producing additional cryptocurrency depends on the existing stock in circulation. Intuitively, if the price of cryptocurrency increases and creates deflation, miners will produce more cryptocurrency due to the high return on it; while if the price of cryptocurrency decreases, since the marginal production cost strictly increases in the aggregate stock of money, miners do not have an incentive to create additional cryptocurrency given the total stock. In both cases, the real balances of cryptocurrency would not remain constant in stationary equilibrium. Thus, the price of cryptocurrency has to be stable, and the inflation rate is zero in a stationary monetary equilibrium. My analysis confirms the conjecture in Hayek (1999) that a purely private arrangement would deliver price stability.

This result is in sharp contrast to models with fiat money, in which the stock of money is exogenously given, e.g., Lagos and Wright (2005) and Rocheteau and Wright (2005). In fiat money economies, there is no incentive problem for the production of fiat money. The inflation rate is determined by the rate of growth of the money stock, and it can be different from zero as long as the stock of fiat money changes over time. However, in the cryptocurrency economy, the money supply is endogenously driven by miners, and the shape of the production cost function determines the relationship between equilibrium prices, aggregate stock, and miners' production incentives.

Further, my result is also in sharp contrast to other types of private money economies, in which the inflation rate must necessarily be different from zero. For example, Fernández-Villaverde and Sanches (2018) claim that a monetary equilibrium with private monies that are issued by profit-

maximizing entrepreneurs, in general, will not deliver price stability. In their private money economy, the cost of producing additional money is independent of the existing stock, e.g., the marginal cost goes to zero as newly produced money goes to zero. In that case, entrepreneurs always have an incentive to create an additional unit of private money, which would eventually violate the transversality condition under price stability. However, in the context of cryptocurrency, because the marginal production cost strictly increases in the stock of money in circulation, which is subject to currency depreciation, miners do not have an incentive to produce cryptocurrency in excess of the flow of currency exogenously lost. Therefore, the price of cryptocurrency remains constant in monetary equilibrium, and the claim about private money in Fernández-Villaverde and Sanches (2018) does not hold in the environment with the cost function satisfying Assumption 2.2. To make my argument explicit, in the next section, I show that the claim of Fernández-Villaverde and Sanches is correct in a version of my model with different assumptions about technology.

3.1.1. Alternative Private Money Economy

In this section, I consider an alternative private money economy, in which the marginal cost of producing an additional unit of money is independent of the aggregate stock and in which the currency depreciation rate is zero.

Suppose the production cost function is convex in the newly produced units of money and satisfying the following assumption.

Assumption 3.1. *The cost function of producing private money,* $c(\delta_t^i) : \mathbb{R} \to \mathbb{R}$*, is increasing, convex, and twice differentiable, s.t.* $\frac{\partial c(\delta_t^i)}{\partial \delta_t^i} > 0$, $\frac{\partial^2 c(\delta_t^i)}{\partial \delta_t^{i2}} > 0$, *and satisfies* $c'(0) = 0$.

In this environment, given the cost function satisfying Assumption 3.1, a miner's production decision only depends on the price of money.

Next, suppose $\kappa = 0$. Then the net circulation of money in each period is only determined by the newly produced units, such that:

$$M_t = M_{t-1} + \Delta_t, \quad \Delta_t \geq 0, \quad M_{-1} \text{ given.} \tag{23}$$

Proposition 3. *Under Assumptions 2.1 and 3.1 and given* $\kappa = 0$*, a stationary monetary equilibrium of private money is inconsistent with price stability.*

Given the new shape of the production cost function, profit-maximizing miners always have an incentive to create an additional unit of money when the money is valued, which would eventually violate the transversality condition under price stability. Thus, if I make the marginal production cost independent of the aggregate stock in my model and set the currency depreciation rate to zero, a monetary equilibrium necessarily has positive inflation. The conjecture of Fernández-Villaverde and Sanches is correct in a version of my model with different assumptions about the production cost function and the currency depreciation. See Appendix C for details.

3.2. Non-Stationary Equilibria

The previous results show that in the cryptocurrency economy, there is a non-monetary stationary equilibrium, i.e., $p^{ss} = z^{ss} = 0$, and a monetary stationary equilibrium, i.e., $p^{ss} > 0, z^{ss} > 0$. In this section, I analyze the non-stationary equilibria and investigate the existence of inflationary equilibrium trajectories.

Proposition 4. *Under Assumptions 2.1 and 2.2, there exists a continuum of equilibria in which the values of cryptocurrency converge to zero.*

Cryptocurrency is intrinsically worthless and is traded because of the liquidity services in decentralized meetings. Agents in the economy form their beliefs and expectations about the value of cryptocurrency in future periods. Proposition 4 shows that cryptocurrency is subject to a self-fulfilling prophecy, even under the existence of a monetary equilibrium with a stable price. For an initial cryptocurrency value less than its steady-state value, there exists an equilibrium path that the values of cryptocurrency depreciate and converge to zero. Along the inflationary equilibrium trajectory, the expected depreciating currency values lead the real balances of cryptocurrency to decline and converge to zero. In this situation, agents' beliefs about the depreciating value of cryptocurrency in the economy can be self-fulfilling.

This result is similar to what happens in models with government-issued fiat money, e.g., Lagos and Wright (2003), in which the stock of money is issued according to a rate of growth. It is also similar to what happens in models with other types of private money, e.g., Fernández-Villaverde and Sanches (2019), in which profit-maximizing agents determine the money supply.

4. Two-Currency Model

To explore the coexistence of cryptocurrency and another intrinsically worthless object—government-issued fiat money—as media of exchange, I extend my cryptocurrency-only model in Section 2 by adding fiat money and multiple decentralized markets, which differ in the currencies that can be used as payment methods.

4.1. Currencies

Let cryptocurrency be indexed by c and fiat money be indexed by m. Cryptocurrency is modeled in the same way as in Section 2.1. Fiat money is issued by the government and is perfectly divisible. Let M_t^m denote the total fiat money stock in period t. Fiat money is supplied according to a deterministic growth rule $\gamma - 1 \in \mathbb{R}$ s.t. $\gamma \equiv \frac{M_t^m}{M_{t-1}^m}$. Changes in fiat money supply are implemented through lump-sum transfers (if $\gamma > 1$) or taxes (if $\gamma < 1$) to buyers in the centralized market.[21] In this paper, I treat γ as an exogenous variable. Let p_t^m denote the value of fiat money per unit in terms of the CM good in period t. Accordingly, the lump-sum transfers/taxes from the government in period t, expressed in terms of the CM good, are $T_t = p_t^m(\gamma - 1)M_{t-1}^m$.

In the two-currency economy, there are several features of cryptocurrency that distinguish it from fiat money. The two currencies differ in their issuers, production costs, supply rules, and degrees of acceptability in decentralized markets.

i. Cryptocurrency is private money and produced by profit-maximizing miners, while fiat money is issued by the government that has sufficient power to tax agents in the economy.
ii. Cryptocurrency is costly to produce, and its production cost strictly increases in both the newly produced units and the existing cryptocurrency stock, while fiat money is costless to produce.
iii. The net circulation of cryptocurrency is endogenously determined by miners' production decisions and the cryptocurrency depreciation, while fiat money is exogenously supplied according to a deterministic growth rule.
iv. Cryptocurrency and fiat money have different degrees of acceptability in decentralized markets, which are specified in the following section.

[21] The government can only tax agents in the centralized market because agents are anonymous and cannot be monitored in the decentralized market. Alternatively, Andolfatto (2013) considers lump-sum tax obligations as a form of debt subject to default. In that case, agents who fail to pay taxes in the centralized market will be excluded from trades in the decentralized market.

4.2. ***Environment***

The monetary environment is similar to that in Section 2. There are three types of infinitely lived agents: *buyers, sellers,* and *miners*, and each of them are populated with a [0,1]-continuum. Time is discrete and continues forever, and each period is divided into two sub-periods.[22]

In the first sub-period, all agents interact in a centralized market. Miners produce cryptocurrency, and buyers and sellers produce the CM good. All agents trade the CM good and adjust their currency portfolios, which comprise fiat money and cryptocurrency holdings. Different from the cryptocurrency-only economy, buyers receive lump-sum transfers/taxes from the government before making their decisions.

In the second sub-period, miners remain idle. Sellers and buyers randomly enter one of the three decentralized markets: DM1, DM2, and DM3, with probabilities α_1, α_2, and α_3, respectively, where $\alpha_{DM} \in [0,1]$ and $\sum_{DM=1}^{3} \alpha_{DM} = 1$, $\forall DM \in \{1,2,3\}$. The DM good is produced and traded in each decentralized market. Search friction, trading process, and agents' preferences and specialization are the same across three decentralized markets. Specifically, in each decentralized market, a buyer is randomly matched with a seller with the probability $\sigma \in (0,1)$ and vice versa. The terms of trade are determined by a take-it-or-leave-it offer by the buyer in each match, and the utility and cost functions of the DM good satisfy Assumption 2.1. With the probability $1-\sigma$, a buyer and a seller are not matched. Then agents proceed to the next period with the same currency portfolios that they carry out of the centralized market.

Three decentralized markets differ in the currencies that can be used as payment methods. Specifically, in DM1, agents can only trade with fiat money; in DM2, agents can only trade with cryptocurrency; and in DM3, agents can trade with any arbitrary mix of the two currencies. Figure 2 summarizes the timing of events in a typical period of the two-currency economy.

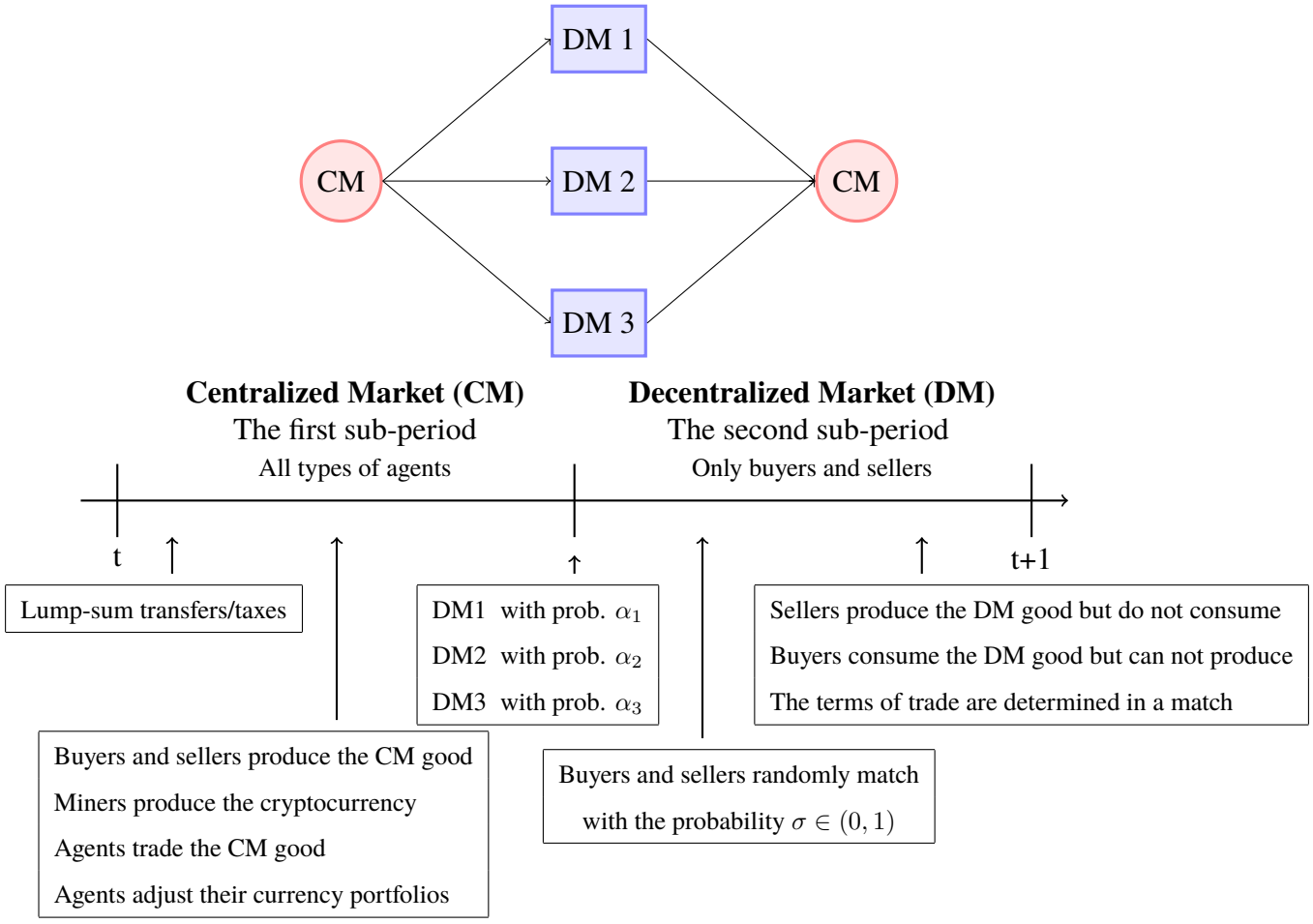
4.3. **Miners**

Miners are only active during the first sub-period. In the centralized market, a typical miner i chooses the consumption of the CM good, x_t^i, produces δ_t^i units of cryptocurrency, and sells all the newly produced units at the price p_t^c right after production. Since miners remain idle in the second sub-period, they do not have an incentive to carry fiat money out of the centralized market. Without loss of generality, I assume that miners do not carry the government-issued money.[23]

[22]The market structure of my two-currency model follows that of the two-currency, two-country search models for international currencies, e.g., Zhang (2014). It is also analogous to the models of competing currencies, e.g., Choi and Rocheteau (2020b), Zhu and Hendry (2019), and Chiu et al. (2020).

[23]Appendix E.2 describes the problem of miners when they are allowed to carry fiat money. In that case, the equilibrium outcomes remain the same as in the main context.

Figure 2: **Timing of Events in a Typical Period with the Two Currencies**



The maximization problem of a typical miner i is represented by:

$$\begin{aligned} \max_{x_t^i, \delta_t^i} \quad & \sum_{t=0}^{\infty} \beta^t x_t^i \\ \text{s.t.} \quad & x_t^i + c(\delta_t^i, M_{t-1}^c) \leq p_t^c \delta_t^i \quad \forall t \\ & x_t^i, \delta_t^i \geq 0 \qquad \forall t \end{aligned} \tag{24}$$

The production cost function of cryptocurrency satisfies Assumption 2.2. Similar to the cryptocurrency-only economy, a miner i's choice of the cryptocurrency production in period t depends only on the value and stock of cryptocurrency, such that

$$\delta_t^i = \max\left[0, f(p_t^c, M_{t-1}^c)\right] \tag{25}$$

The aggregate new cryptocurrency in period t, Δ_t, is the same as (18) with $p_t = p_t^c$ and $M_t = M_t^c$.

4.4. Buyers and Sellers

Next, I describe the problems faced by buyers and sellers in the two-currency economy.

4.4.1. The Centralized Market Problems

A typical buyer b and seller s begin a period with their currency portfolios from the last period, $\mathbf{m}_{t-1}^j = (m_{t-1}^{m,j}, m_{t-1}^{c,j})$, which comprise $m_{t-1}^{m,j}$ units of fiat money and $m_{t-1}^{c,j}$ units of cryptocurrency, $j \in \{b, s\}$. Due to different trading histories in decentralized markets, agents begin a period with different currency portfolios. In the centralized market, a certain fraction, $\kappa \in (0, 1)$, of the cryptocurrency holdings is lost, and buyers receive lump-sum transfers/taxes from the government. In the first sub-period, a buyer and seller choose their net consumption of the CM good, x_t^b, x_t^s, and currency portfolios, $\mathbf{m}_t^b, \mathbf{m}_t^s$, to bring forward to the next sub-period, respectively.

Let $W_t^j(\mathbf{m}_{t-1}^j)$ denote the value function of an agent beginning a period with currency portfolio, $\mathbf{m}_{t-1}^j = (m_{t-1}^{m,j}, m_{t-1}^{c,j}) \in \mathbb{R}_+^2$, and $V_t^j(\mathbf{m}_t^j)$ denote the value function of an agent beginning the second sub-period with the chosen currency portfolio, $\mathbf{m}_t^j = (m_t^{m,j}, m_t^{c,j}) \in \mathbb{R}_+^2$, $j \in \{b, s\}$. The maximization problems of a typical buyer and seller in the centralized market are represented by:

$$W_t^b(\mathbf{m_{t-1}^b}) = \max_{x_t^b, \mathbf{m_t^b}} \; x_t^b + V_t^b(\mathbf{m_t^b}) \quad s.t. \quad x_t^b + \mathbf{p_t m_t^b} = p_t^m m_{t-1}^{m,b} + (1-\kappa) p_t^c m_{t-1}^{c,b} + T_t \tag{26}$$

$$W_t^s(\mathbf{m_{t-1}^s}) = \max_{x_t^s, \mathbf{m_t^s}} \; x_t^s + V_t^s(\mathbf{m_t^s}) \quad s.t. \quad x_t^s + \mathbf{p_t m_t^s} = p_t^m m_{t-1}^{m,s} + (1-\kappa) p_t^c m_{t-1}^{c,s} \tag{27}$$

where $\mathbf{p}_t = (p_t^m, p_t^c) \in \mathbb{R}_+^2$ is the price vector of fiat money and cryptocurrency. The CM value functions (26)-(27) can be rearranged as:

$$W_t^j(\mathbf{m_{t-1}^j}) = p_t^m m_{t-1}^{m,j} + (1-\kappa) p_t^c m_{t-1}^{c,j} + W_t^j(0,0) \tag{28}$$

where $W_t^b(0,0) = T_t + \max_{\mathbf{m_t^b} \in \mathbb{R}_+^2} -\mathbf{p_t m_t^b} + V_t^b(\mathbf{m_t^b})$ and $W_t^s(0,0) = \max_{\mathbf{m_t^s} \in \mathbb{R}_+^2} -\mathbf{p_t m_t^s} + V_t^s(\mathbf{m_t^s})$, $j \in \{b, s\}$. Similar to the cryptocurrency-only economy, there is no wealth effect on an agent's choice of currency portfolio. The choice of $\mathbf{m}_t^j$, $j \in \{b, s\}$, is independent of lump-sum transfers/taxes from the government, the initial currency portfolio when entering the centralized market, and the cryptocurrency loss.

4.4.2. ***The Decentralized Markets Problems***

In the second sub-period, with the chosen currency portfolios $\mathbf{m}_t^j,\ j \in \{b, s\}$, a buyer and seller randomly enter the DM1, DM2, and DM3 with probabilities α_1, α_2, and α_3, respectively. The DM problems for a typical buyer and seller are represented by:

$$\begin{aligned} V_t^b(\mathbf{m_t^b}) = \max_{(q_t^1,d_t^{1,m}),(q_t^2,d_t^{2,c}),(q_t^3,d_t^{3,m},d_t^{3,c})} & \alpha_1\{\sigma[u(q_t^1) + \beta W_{t+1}^b(m_t^{m,b} - d_t^{1,m}, m_t^{c,b})] + (1-\sigma)\beta W_{t+1}^b(\mathbf{m}_t^b)\} \\ & + \alpha_2\{\sigma[u(q_t^2) + \beta W_{t+1}^b(m_t^{m,b}, m_t^{c,b} - d_t^{2,c})] + (1-\sigma)\beta W_{t+1}^b(\mathbf{m}_t^b)\} \\ & + \alpha_3\{\sigma[u(q_t^3) + \beta W_{t+1}^b(m_t^{m,b} - d_t^{3,m}, m_t^{c,b} - d_t^{3,c})] + (1-\sigma)\beta W_{t+1}^b(\mathbf{m_t^b})\} \end{aligned} \tag{29}$$

$$\begin{aligned} V_t^s(\mathbf{m_t^s}) = & \alpha_1\{\sigma[-\omega(q_t^1) + \beta W_{t+1}^s(m_t^{m,s} + d_t^{1,m}, m_t^{c,s})] + (1-\sigma)\beta W_{t+1}^s(\mathbf{m}_t^s)\} \\ & + \alpha_2\{\sigma[-\omega(q_t^2) + \beta W_{t+1}^s(m_t^{m,s}, m_t^{c,s} + d_t^{2,c})] + (1-\sigma)\beta W_{t+1}^s(\mathbf{m}_t^s)\} \\ & + \alpha_3\{\sigma[-\omega(q_t^3) + \beta W_{t+1}^s(m_t^{m,s} + d_t^{3,m}, m_t^{c,s} + d_t^{3,c})] + (1-\sigma)\beta W_{t+1}^s(\mathbf{m_t^s})\} \end{aligned} \tag{30}$$

where $(q_t^1, d_t^{1,m}), (q_t^2, d_t^{2,c})$, and $(q_t^3, d_t^{3,m}, d_t^{3,c})$ denote the terms of trade in the DM1, DM2, and DM3, respectively. In particular, $q_t^1, q_t^2, q_t^3 \in \mathbb{R}_+$ denote the quantity of the DM good traded in each decentralized market, and $d_t^{1,m}, d_t^{2,c}, d_t^{3,m}, d_t^{3,c} \in \mathbb{R}_+$ denote the transfer of the corresponding currency from the buyer to the seller. Specifically, in DM1, the buyer is only allowed to make offers on fiat money, $d_t^{1,m}$; in DM2, the buyer is only allowed to make offers on cryptocurrency, $d_t^{2,c}$; and in DM3, the buyer is allowed to make offers for any arbitrary mix of the two currencies, $(d_t^{3,m}, d_t^{3,c})$.

In each decentralized market, if a buyer matches with a seller and trade happens, then the buyer gains utilities from consuming DM goods, while the seller produces DM goods with some costs, and both of their currency portfolios change after the buyer makes transfers to the seller. In each match, the terms of trade are determined by a take-it-or-leave-it offer by a buyer. Depending on the decentralized market that the buyer enters, the optimal offer is given by the solution to:

$$\begin{aligned} \text{In DM1:} \quad & \max_{q_t^1, d_t^1} \quad u(q_t^1) + \beta W_{t+1}^b(m_t^{m,b} - d_t^{1,m}, m_t^{c,b}) \\ & s.t. \quad -\omega(q_t^1) + \beta W_{t+1}^s(m_t^{m,s} + d_t^{1,m}, m_t^{c,s}) \geq \beta W_{t+1}^s(m_t^{m,s}, m_t^{c,s}) \\ & \quad d_t^{1,m} \leq m_t^{m,b} \end{aligned} \tag{31}$$

$$\begin{aligned} \text{In DM2:} \quad & \max_{q_t^2, d_t^2} \quad u(q_t^2) + \beta W_{t+1}^b(m_t^{m,b}, m_t^{c,b} - d_t^{2,c}) \\ & s.t. \quad -\omega(q_t^2) + \beta W_{t+1}^s(m_t^{m,s}, m_t^{c,s} + d_t^{2,c}) \geq \beta W_{t+1}^s(m_t^{m,s}, m_t^{c,s}) \\ & \quad d_t^{2,c} \leq m_t^{c,b} \end{aligned} \tag{32}$$

$$\text{In DM3:} \quad \max_{q_t^3, d_t^{3,m}, d_t^{3,c}} \quad u(q_t^3) + \beta W_{t+1}^b(m_t^{m,b} - d_t^{3,m}, m_t^{c,b} - d_t^{3,c})$$
$$s.t. \quad -\omega(q_t^3) + \beta W_{t+1}^s(m_t^{m,s} + d_t^{3,m}, m_t^{c,s} + d_t^{3,c}) \geq \beta W_{t+1}^s(m_t^{m,s}, m_t^{c,s}) \tag{33}$$
$$d_t^{3,m} \leq m_t^{m,b}, d_t^{3,c} \leq m_t^{c,b}$$

The first constraint in each problem above is the seller's participation constraint and the second one is the buyer's liquidity constraint.

According to (28), problems (31)-(33) can be simplified as follows.

$$\text{In DM1:} \quad \max_{q_t^1, d_t^{1,m}} \quad u(q_t^1) - \beta p_{t+1}^m d_t^{1,m} \tag{34}$$
$$s.t. \quad -\omega(q_t^1) + \beta p_{t+1}^m d_t^{1,m} \geq 0, \quad d_t^{1,m} \leq m_t^{m,b}$$

$$\text{In DM2:} \quad \max_{q_t^2, d_t^{2,c}} \quad u(q_t^2) - \beta p_{t+1}^c (1-\kappa) d_t^{2,c} \tag{35}$$
$$s.t. \quad -\omega(q_t^2) + \beta p_{t+1}^c (1-\kappa) d_t^{2,c} \geq 0, \quad d_t^{2,c} \leq m_t^{c,b}$$

$$\text{In DM3:} \quad \max_{q_t^3, d_t^{3,m}, d_t^{3,c}} \quad u(q_t^3) - \beta p_{t+1}^m d_t^{3,m} - \beta p_{t+1}^c (1-\kappa) d_t^{3,c}$$
$$s.t. \quad -\omega(q_t^3) + \beta p_{t+1}^m d_t^{3,m} + \beta p_{t+1}^c (1-\kappa) d_t^{3,c} \geq 0 \tag{36}$$
$$d_t^{3,m} \leq m_t^{m,b}, d_t^{3,c} \leq m_t^{c,b}$$

Similar to the cryptocurrency-only economy, if a buyer can afford q^* using the currencies that are accepted as payment methods in that decentralized market, then the buyer would pay for q^*, i.e., $d_t^{1,m} = m_t^{m*} = \frac{\omega(q^*)}{\beta p_{t+1}^m}$, $d_t^{2,c} = m_t^{c*} = \frac{\omega(q^*)}{\beta p_{t+1}^c (1-\kappa)}$, $(d_t^{3,m}, d_t^{3,c}) = (\hat{m}_t^{m,b}, \hat{m}_t^{c,b})$ s.t. $\omega(q^*) = \beta(p_{t+1}^m \hat{m}_t^{m,b} + p_{t+1}^c (1-\kappa)\hat{m}_t^{c,b})$. Otherwise, the buyer would spend all the currencies that can be used in that market to purchase the DM good. More specifically, in DM1: $d^{1,m} = m_t^{m,b}, q_t^1 = \omega^{-1}(\beta p_{t+1}^m m_t^{m,b}) < q^*$; in DM2: $d^{2,c} = m_t^{c,b}, q_t^2 = \omega^{-1}(\beta p_{t+1}^c (1-\kappa) m_t^{c,b}) < q^*$; and in DM3: $(d_t^{3,m}, d_t^{3,c}) = (m_t^{m,b}, m_t^{c,b}), q_t^3 = \omega^{-1}(\beta p_{t+1}^m m_t^{m,b} + \beta p_{t+1}^c (1-\kappa) m_t^{c,b}) < q^*$, which implies that cryptocurrency and fiat money are perfect substitutes in DM3 in equilibrium, in the sense that agents are indifferent about the two currencies.

Solutions to (34)-(36) are summarized in the following Lemma.

Lemma 4.1. *The solutions to the terms of trade (q_t^{DM}, d_t^{DM}) in the decentralized market DM, $DM \in \{1,2,3\}$, are given by:*

$$(q_t^{DM}, d_t^{DM}) = \begin{cases} q_t^1 = q^*, \;\; d_t^{1,m} = m_t^{m*} = \frac{\omega(q^*)}{\beta p_{t+1}^m} \\ q_t^2 = q^*, \;\; d_t^{2,c} = m_t^{c*} = \frac{\omega(q^*)}{\beta p_{t+1}^c (1-\kappa)} \\ q_t^3 = q^*, \;\; (d_t^{3,m}, d_t^{3,c}) = (\hat{m}_t^{m,b}, \hat{m}_t^{c,b}) \\ \qquad\qquad s.t. \;\; \omega(q^*) = \beta(p_{t+1}^m \hat{m}_t^{m,b} + p_{t+1}^c (1-\kappa)\hat{m}_t^{c,b}) \end{cases} \quad if \;\; A_{DM,t} \geq \omega(q^*)$$

$$(q_t^{DM}, d_t^{DM}) = \begin{cases} q_t^1 = \hat{q}_t^1 = \omega^{-1}(A_{1,t}), \;\; d_t^{1,m} = m_t^{m,b} \\ q_t^2 = \hat{q}_t^2 = \omega^{-1}(A_{2,t}), \;\; d_t^{2,c} = m_t^{c,b} \\ q_t^3 = \hat{q}_t^3 = \omega^{-1}(A_{3,t}), \;\; (d_t^{3,m}, d_t^{3,c}) = (m_t^{m,b}, m_t^{c,b}) \end{cases} \quad if \;\; A_{DM,t} < \omega(q^*)$$

where $A_{DM,t}$ denotes the total value of assets that are used for trading in the $DM \in \{1,2,3\}$ and in period t, such that $A_{1,t} = \beta p_{t+1}^m m_t^{m,b}$; $A_{2,t} = \beta p_{t+1}^c (1-\kappa) m_t^{c,b}$; $A_{3,t} = \beta(p_{t+1}^m m_t^{m,b} + (1-\kappa)p_{t+1}^c m_t^{c,b})$. The DM output $q^* = argmax\,[u(q_t) - \omega(q_t)]$, and $\hat{q}_t^{DM} < q^*$ when $A_{DM,t} < \omega(q^*)$, $\forall\; DM \in \{1,2,3\}$.

*4.4.3. **The Optimal Currency Portfolio***

Next, following Lemma 4.1 and (28), the optimal currency portfolios of a buyer and seller are given by the solutions to:

$$W_t^b(\mathbf{m}_{t-1}^b) = \max_{m_t^{m,b}, m_t^{c,b} \in \mathbb{R}_+^2} - (p_t^m - \beta p_{t+1}^m) m_t^{m,b} \; - (p_t^c - \beta(1-\kappa)p_{t+1}^c) m_t^{c,b} + v_t^{1,b}(m_t^{m,b}) + v_t^{2,b}(m_t^{c,b}) + v_t^{3,b}(\mathbf{m}_t^b) \tag{37}$$

$$\begin{aligned} \textit{where} \quad v_t^{1,b}(m_t^{m,b}) &= \alpha_1 \sigma[u(q_t^1(m_t^{m,b})) - \beta p_{t+1}^m d_t^{1,m}(m_t^{m,b})] \\ v_t^{2,c}(m_t^{c,b}) &= \alpha_2 \sigma[u(q_t^2(m_t^{c,b})) - \beta p_{t+1}^c (1-\kappa) d_t^{2,c}(m_t^{c,b})] \\ v_t^{3,b}(\mathbf{m}_t^b) &= \alpha_3 \sigma[u(q_t^3(\mathbf{m}_t^b)) - \beta p_{t+1}^m d_t^{3,m}(\mathbf{m}_t^b) - \beta p_{t+1}^c (1-\kappa) d_t^{3,c}(\mathbf{m}_t^b)] \end{aligned}$$

$$W_t^s(\mathbf{m}_{t-1}^s) = \max_{m_t^{m,s}, m_t^{c,s} \in \mathbb{R}_+^2} - (p_t^m - \beta p_{t+1}^m) m_t^{m,s} \; - (p_t^c - \beta(1-\kappa)p_{t+1}^c) m_t^{c,s} + 0 + 0 + 0 \tag{38}$$

The first two terms on the RHS of (37)-(38) represent the cost of carrying fiat money and cryptocurrency to the next period, while the last three terms represent the expected surplus of an agent in each decentralized market. Since buyers are the ones to make the take-it-or-leave-it offer, they take all the gains and sellers have no surplus from trades in any decentralized market.

From (37)-(38), agents choose the optimal currency portfolios to maximize their expected surplus from using them in the second sub-period net of the cost of carrying each currency. Cryptocurrency is costly to carry when $p_t^c > \beta p_{t+1}^c(1-\kappa)$, while fiat money is costly to carry when $p_t^m > \beta p_{t+1}^m$. The optimal currency portfolios for a buyer and seller can be obtained by taking the F.O.C. of (37)-(38) with respect to $[m^{m,j}]$ and $[m^{c,j}]$, $j \in \{b, s\}$.

Lemma 4.2. *The optimal currency portfolios for a buyer and seller must satisfy:*

$$[m_t^{m,b}] \quad \frac{p_t^m}{\beta p_{t+1}^m} - 1 \geq \alpha_1 \sigma L(p_{t+1}^m m_t^{m,b}) + \alpha_3 \sigma L(p_{t+1}^m m_t^{m,b} + (1-\kappa) p_{t+1}^c m_t^{c,b})$$

$$\text{“}=\text{”} \textit{ if } \quad m_t^{m,b} > 0 \tag{39}$$

$$[m_t^{c,b}] \quad \frac{p_t^c}{\beta p_{t+1}^c(1-\kappa)} - 1 \geq \alpha_2 \sigma L(p_{t+1}^c(1-\kappa) m_t^{c,b}) + \alpha_3 \sigma L(p_{t+1}^m m_t^{m,b} + (1-\kappa) p_{t+1}^c m_t^{c,b})$$

$$\text{“}=\text{”} \textit{ if } \quad m_t^{c,b} > 0 \tag{40}$$

$$\textit{where } L(X) = \begin{cases} 0 & \textit{if} \quad \beta X \geq \omega(q^*) \\ \{\frac{u'}{\omega'} \circ \omega^{-1}(\beta X) - 1\} > 0 & \textit{if} \quad \beta X < \omega(q^*) \end{cases}$$

$$[m_t^{m,s}] \quad -p_t^m + \beta p_{t+1}^m \leq 0 \qquad \text{“}=\text{”} \quad \textit{if} \quad m_t^{m,s} > 0 \tag{41}$$

$$[m_t^{c,s}] \quad -p_t^c + \beta p_{t+1}^c(1-\kappa) \leq 0 \qquad \text{“}=\text{”} \quad \textit{if} \quad m_t^{c,s} > 0 \tag{42}$$

The term $L(\cdot)$ represents the liquidity premium. It equals to zero when buyers can afford q^* in a decentralized meeting, and is strictly greater than zero when buyers can not afford q^*. From (41)-(42), a seller will not carry any unit of fiat money or cryptocurrency out of the centralized market if that currency is costly to carry.

Lemma 4.2 states that if an agent chooses to hold one currency, the marginal cost of carrying that currency into the next sub-period must equal the expected marginal payoff from using it to facilitate all kinds of transactions in decentralized markets. Since sellers have no surplus from trades in all decentralized markets, there is no strict incentive for them to carry currency portfolios forward to the second sub-period.

5. Equilibrium

This section describes the equilibrium conditions of the two-currency economy and analyzes the coexistence of cryptocurrency and fiat money.

Definition 4. *Given γ, an equilibrium is a set of decision rules in the centralized market $\{x_t^b, \mathbf{m}_t^b, x_t^s, \mathbf{m}_t^s, x_t^i, \delta_t^i\}_{t=0}^{\infty}$, the terms of trade in each decentralized market $\{(q_t^1, d_t^{1,m}), (q_t^2, d_t^{2,c}), (q_t^3, d_t^{3,m}, d_t^{3,c})\}_{t=0}^{\infty}$, sequences of values of two currencies $\{p_t^c, p_t^m\}_{t=0}^{\infty}$, and the aggregate supply of cryptocurrency $\{M_t^c\}_{t=0}^{\infty}$, such that for all $t \geq 0$: $\{x_t^b, \mathbf{m}_t^b, x_t^s, \mathbf{m}_t^s\}$ solve problems (26)-(27) and (29)-(30); $\{x_t^i, \delta_t^i\}$ solve problem (24); $\{(q_t^1, d_t^{1,m}), (q_t^2, d_t^{2,c}), (q_t^3, d_t^{3,m}, d_t^{3,c})\}$ solve problems (34)-(36); as well as market clearing for centralized good, fiat money, and cryptocurrency, and the cryptocurrency law of motion and transversality conditions are satisfied.*

Definition 5. *A stationary equilibrium is an equilibrium in which the real balances of cryptocurrency and fiat money are constant, i.e., $p_t^m M_t^m = p_{t+1}^m M_{t+1}^m = z_m,\ p_t^c M_t^c = p_{t+1}^c M_{t+1}^c = z_c, \forall t$.*

In what follows, I analyze the stationary equilibrium in the two-currency economy. My focus is on examining whether cryptocurrency—an asset that is costly to produce—can coexist with fiat money—an asset that is costless to produce—in the economy.

Suppose that, in general, the supplies of fiat money and cryptocurrency grow at constant rates, such that $M_{t+1}^m = \gamma M_t^m$ where $\gamma > \beta$ and $M_{t+1}^c = (1+\mu) M_t^c$ where $\mu > -\kappa$. Since sellers and miners have no incentive to carry currencies out of the centralized market, following market clear conditions and Lemma 4.2, the equilibrium conditions can be expressed as follows.

$$i_m \geq \alpha_1 \sigma L(\frac{z_m}{\gamma}) + \alpha_3 \sigma L(\frac{z_m}{\gamma} + \frac{(1-\kappa) z_c}{1+\mu}) \qquad \text{“}=\text{”} \text{ if } z_m > 0 \tag{43}$$

$$i_c \geq \alpha_2 \sigma L(\frac{(1-\kappa) z_c}{1+\mu}) + \alpha_3 \sigma L(\frac{z_m}{\gamma} + \frac{(1-\kappa) z_c}{1+\mu}) \qquad \text{“}=\text{”} \text{ if } z_c > 0 \tag{44}$$

where $i_m = \frac{p_t^m}{\beta p_{t+1}^m} - 1$ and $i_c = \frac{p_t^c}{\beta p_{t+1}^c (1-\kappa)} - 1$ denote the cost of carrying fiat money and cryptocurrency, respectively, which depend on the rate of return, time preference, and the currency depreciation rate.[24] According to (43)-(44), a currency is not valued when the cost of carrying it outweighs the expected payoff of using it in decentralized markets. The government can affect an agent's incentive to make currency portfolio choices through changing the monetary policy on the growth rule of the fiat money supply.

[24]The term $1 + i_m$ can be interpreted as the interest rate on an illiquid nominal bond dominated in fiat money, see, e.g., Zhu and Hendry (2019).

There are four types of currency regimes in stationary equilibrium: no currency is valued ($z_m = z_c = 0$); only fiat money is valued ($z_m > 0,\ z_c = 0$); only cryptocurrency is valued ($z_m = 0,\ z_c > 0$); and both currencies are valued ($z_m > 0,\ z_c > 0$). This is similar to multiple fiat currencies models, e.g., Camera et al. (2004) and Engineer (2000). Next, I explore the existence conditions of these currency regimes given γ, μ, and the fundamentals of the economy, following the approaches of Zhang (2014) and Zhu and Hendry (2019).

A non-monetary stationary equilibrium, in which no currency is valued, occurs when both currencies are too costly to hold, i.e., $i_m \geq \alpha_1\sigma L(0) + \alpha_3\sigma L(0)$ and $i_c \geq \alpha_2\sigma L(0) + \alpha_3\sigma L(0)$. Accordingly, given the parameters and functional forms of the model, a unique non-monetary stationary equilibrium, $z_m = z_c = 0$, exists, so long as $\gamma \geq \tilde{\gamma}$ and $(1+\mu) \geq 1+\tilde{\mu}$, where $\tilde{\gamma}$ and $\tilde{\mu}$ are given by:

$$\frac{\tilde{\gamma}}{\beta} - 1 = \alpha_1\sigma L(0) + \alpha_3\sigma L(0) \tag{45}$$

$$\frac{1+\tilde{\mu}}{\beta(1-\kappa)} - 1 = \alpha_2\sigma L(0) + \alpha_3\sigma L(0) \tag{46}$$

A stationary equilibrium in which only fiat money is valued occurs when cryptocurrency is too costly to hold while fiat money is not. That is, $i_m = \alpha_1\sigma L(z_m/\gamma) + \alpha_3\sigma L(z_m/\gamma)$ and $i_c \geq \alpha_2\sigma L(0) + \alpha_3\sigma L(z_m/\gamma)$. This might happen when the size of the markets in which sellers accept cryptocurrency for transactions is too small, or when the cryptocurrency depreciation rate is large, or when the rate of return on cryptocurrency is sufficiently low. Thus, a stationary equilibrium in which $z_m > 0$ and $z_c = 0$ exists, so long as $\beta < \gamma < \tilde{\gamma}$ and $1+\mu \geq 1+\bar{\mu}$, where $\tilde{\gamma}$ is from (45) and $\bar{\mu}$ is given by:

$$\frac{1+\bar{\mu}}{\beta(1-\kappa)} - 1 = \alpha_2\sigma L(0) + \frac{\alpha_3}{\alpha_1+\alpha_3}\left(\frac{\gamma}{\beta} - 1\right) \tag{47}$$

Symmetrically, a stationary equilibrium in which only cryptocurrency is valued, i.e., $z_m = 0$ and $z_c > 0$, exists so long as $\gamma \geq \bar{\gamma}$ and $1-\kappa < 1+\mu < 1+\tilde{\mu}$, where $1+\tilde{\mu}$ is from (46) and $\bar{\gamma}$ is given by:

$$\frac{\bar{\gamma}}{\beta} - 1 = \alpha_1\sigma L(0) + \frac{\alpha_3}{\alpha_2+\alpha_3}\left(\frac{1+\mu}{\beta(1-\kappa)} - 1\right) \tag{48}$$

Lastly, a stationary equilibrium in which both currencies are valued, i.e., $z_m > 0$ and $z_c > 0$, exists so long as $\beta < \gamma < \bar{\gamma}$ and $1-\kappa < 1+\mu < 1+\bar{\mu}$, where $\bar{\gamma}$ and $\bar{\mu}$ are given by (48) and (47), respectively.

5.1. Coexistence

Next, I characterize the stationary equilibrium in which both currencies are valued in the economy.

Proposition 5. *Given γ and $\alpha_{DM} \in (0,1)\ \forall DM \in \{1,2,3\}$, and under Assumptions 2.1 and 2.2, there exists a stationary equilibrium in which both cryptocurrency and fiat money are valued, and in which the price of cryptocurrency is constant and that of fiat money changes at a constant rate s.t. $p^m_{t+1} = \frac{1}{\gamma} p^m_t$, so long as $\beta < \gamma < \bar{\gamma} \equiv \beta\alpha_1\sigma L(0) + \frac{\alpha_3}{\alpha_2+\alpha_3}(\frac{1}{1-\kappa} - \beta) + \beta$ and $0 < \hat{\mu} \equiv (\alpha_2\sigma L(0) + 1)\beta(1-\kappa) - 1$. The equilibrium outcomes are characterized by:*

$$\frac{\gamma - \beta}{\sigma\beta} = \alpha_1[\frac{u' \circ \omega^{-1}(\beta\frac{z_m}{\gamma})}{\omega' \circ \omega^{-1}(\beta\frac{z_m}{\gamma})} - 1] + \alpha_3[\frac{u' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\kappa)))}{\omega' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\kappa)))} - 1] \tag{49}$$

$$\frac{1 - \beta(1-\kappa)}{\sigma\beta(1-\kappa)} = \alpha_2[\frac{u' \circ \omega^{-1}(\beta z_c(1-\kappa))}{\omega' \circ \omega^{-1}(\beta z_c(1-\kappa))} - 1] + \alpha_3[\frac{u' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\kappa)))}{\omega' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\kappa)))} - 1] \tag{50}$$

$$f(p_c^{ss}, M_c^{ss}) = \kappa M_c^{ss} \tag{51}$$

$$q_1^{ss} = \omega^{-1}(\beta\frac{z_m}{\gamma}) \tag{52}$$

$$q_2^{ss} = \omega^{-1}(\beta z_c(1-\kappa)) \tag{53}$$

$$q_3^{ss} = \omega^{-1}(\beta\frac{z_m}{\gamma} + \beta z_c(1-\kappa)) \tag{54}$$

$$\Delta^{ss} = \kappa M_c^{ss} \tag{55}$$

Given the forms of $u(\cdot), \omega(\cdot)$, and parameters of the economy, under Assumptions 2.1 and 2.2, there exists a set of equilibrium outcomes that satisfy (49)-(55) so long as $\beta < \gamma < \bar{\gamma}$ and $0 < \hat{\mu}$, where $\bar{\gamma}$ is obtained from (48) with $\mu = 0$, and $\hat{\mu}$ is given by (47) with $\gamma = \beta$.

Different from what happens in traditional two-fiat money models, in which the rates of return on two fiat currencies must be the same if both currencies are in circulation, e.g., Kareken and Wallace (1981), cryptocurrency and fiat money can coexist in equilibrium regardless of their rates of return. This is driven by the assumption that the two currencies have different degrees of acceptability in decentralized markets. Since each currency is essential in some meetings, agents will hold both currencies to smooth their consumption in all decentralized meetings, even if one has a higher inflation rate. Therefore, a low-return currency can coexist with a high-return currency, so long as neither currency is too costly to carry.

Moreover, my two-currency model has a novelty compared to other models of multiple competing currencies with payment acceptability constraints, such as a model of fiat monies, e.g., Zhang

(2014), and a model of private and fiat monies, e.g., Zhu and Hendry (2019). In their models, the cost of carrying one currency is tied with the exogenous growth rate of the money supply. However, in my model, the cost of carrying cryptocurrency depends not only on the exogenous parameters, such as currency depreciation, but also on the endogenous production decisions of miners, which rely on the production cost function and further affect the price path of cryptocurrency in equilibrium. That is because miners endogenously determine the supply of cryptocurrency, and the shape of the cost function determines the relationship between equilibrium prices, aggregate stock, and miners' production incentives through their profit maximization problems. Given the assumption that the marginal cost of producing money strictly increases in the existing stock in circulation, the price and stock of cryptocurrency must remain constant in equilibrium with the coexistence of two currencies.[25] In the next section, I explore how the model fundamentals affect the two currencies.

5.1.1. Comparative Statics

Following Proposition 5, the real value of fiat money is interdependent with that of cryptocurrency. The government monetary policy can affect the value of cryptocurrency, and hence, affect the quantity of DM good traded with cryptocurrency. Intuitively, buyers can make offers on any arbitrary mix of the two currencies in DM3. As the fiat money inflates (i.e., γ increases), it becomes more costly to use fiat money. Then agents would demand less for fiat money and instead substitute into cryptocurrency, which decreases the real value of fiat money and increases that of cryptocurrency. As a monetary equilibrium with coexistence will be consistent with a zero inflation rate in cryptocurrency, the competition with cryptocurrency restricts the government's ability to over-issue fiat money to raise the inflation tax.

In addition, if cryptocurrency is lost at a higher rate (i.e., κ increases), or if the marginal cost of producing cryptocurrency diminishes (i.e., $\frac{\partial c(\delta,M)}{\partial \delta}$ decreases), the cost of carrying cryptocurrency increases.[26] Accordingly, agents would demand less for cryptocurrency and demand more for fiat money in decentralized meetings, which decreases the real value of cryptocurrency and increases that of fiat money. Moreover, as κ increases, the region of parameter $\bar{\gamma}$ increases. Then both currencies would still be valued in equilibrium when the government issues fiat money at a higher rate, as long as the new growth rate is less than the new parameter region $\bar{\gamma}$.

[25] Appendix D presents a two-currency economy where both cryptocurrency and fiat money are exogenously supplied. I show that unlike the economy with endogenously determined cryptocurrency, an economy with exogenously supplied cryptocurrency cannot have an analog of the equilibrium in which the price of cryptocurrency must remain constant.

[26] From the miner's profit maximization problem, the amount of newly produced cryptocurrency in period t is determined by $p_t^c = \frac{\partial c(\delta_t^i, M_{t-1}^c)}{\partial \delta_t^i}$. Taking the functional form in Example 2.1: $\frac{\partial c(\delta_t^i, M_{t-1}^c)}{\partial \delta_t^i} = DM_{t-1}^c + 2B\delta_t^i$ and $\Delta_t = \frac{p_t^c - DM_{t-1}^c}{2B}$. When $\frac{\partial c(\delta_t^i, M_{t-1}^c)}{\partial \delta_t^i}$ diminishes, i.e., $D \downarrow$ or $B \downarrow$, Δ_t and M_t^c increase, which increases the cost of carrying cryptocurrency in equilibrium.

Further, consider the expected payoff of using currencies in decentralized meetings. As the acceptability degree of one currency gets larger, that currency becomes more useful in decentralized markets and thus has a higher expected payoff from using it. Then agents would demand more for that currency and the real value of it would increase. The following table summarizes the effects of the cost of carrying each currency and the market size on the real values of the two currencies. Calculations are provided in Appendix G. In the next section, I explore the equilibrium outcomes with coexistence of two currencies under special cases in terms of the market sizes.

Table 1: Comparative Statics

	i_m	i_c	α_1	α_2	α_3
z_m	$\frac{\partial z_m}{\partial i_m} < 0$	$\frac{\partial z_m}{\partial i_c} > 0$	$\frac{\partial z_m}{\partial \alpha_1} > 0$	$\frac{\partial z_m}{\partial \alpha_2} < 0$	$\frac{\partial z_m}{\partial \alpha_3} > 0$
z_c	$\frac{\partial z_c}{\partial i_m} > 0$	$\frac{\partial z_c}{\partial i_c} < 0$	$\frac{\partial z_c}{\partial \alpha_1} < 0$	$\frac{\partial z_c}{\partial \alpha_2} > 0$	$\frac{\partial z_c}{\partial \alpha_3} > 0$

6. Special Cases with Two Decentralized Markets

In this section, I explore the coexistence of cryptocurrency and fiat money under the following cases: $1)$ when there are completely segmented decentralized markets; $2)$ when cryptocurrency has an inherent advantage relative to fiat money in markets; $3)$ when fiat money has an inherent advantage relative to cryptocurrency in markets.

6.1. Completely Segmented Markets

In the first case, suppose there are only two decentralized markets in the economy: DM1 and DM2, i.e., $\alpha_1, \alpha_2 \in (0,1),\ \alpha_1 + \alpha_2 = 1$, and $\alpha_3 = 0$. That is, agents are only allowed to trade with fiat money in DM1 and trade with cryptocurrency in DM2. Equilibrium outcomes (43)-(44) can be expressed as follows.

$$i_m \ \geq \ \alpha_1 \sigma L(\frac{z_m}{\gamma}) \qquad \text{“} = \text{” if } \ z_m > 0 \tag{56}$$

$$i_c \ \geq \ \alpha_2 \sigma L(\frac{z_c(1-\kappa)}{1+\mu}) \qquad \text{“} = \text{” if } \ z_c > 0 \tag{57}$$

For a currency to be circulating in the economy, the cost of carrying an additional unit of that currency must equal the expected payoff of using it in decentralized meetings.

Proposition 6. *Given γ and $\{\alpha_1, \alpha_2, \alpha_3\}$ s.t. $\alpha_1, \alpha_2 \in (0,1)$, $\alpha_1 + \alpha_2 = 1$, and $\alpha_3 = 0$, under Assumptions 2.1 and 2.2, there exists a unique stationary equilibrium in which both cryptocurrency and fiat money are valued, and in which the price of cryptocurrency is constant and that of fiat money changes at a constant rate s.t. $p^m_{t+1} = \frac{1}{\gamma} p^m_t$, so long as $\beta < \gamma < \bar{\gamma} \equiv \beta\alpha_1\sigma L(0) + \beta$ and $0 < \bar{\mu} \equiv (\alpha_2\sigma L(0) + 1)\beta(1-\kappa) - 1$. The equilibrium outcomes are characterized by:*

$$\frac{\gamma - \beta}{\sigma\beta} = \alpha_1 [\frac{u' \circ \omega^{-1}(\beta \frac{z_m}{\gamma})}{\omega' \circ \omega^{-1}(\beta \frac{z_m}{\gamma})} - 1] \tag{58}$$

$$\frac{1 - \beta(1-\kappa)}{\sigma\beta(1-\kappa)} = \alpha_2 [\frac{u' \circ \omega^{-1}(\beta z_c(1-\kappa))}{\omega' \circ \omega^{-1}(\beta z_c(1-\kappa))} - 1] \tag{59}$$

$$f(p^{ss}_c, M^{ss}_c) = \kappa M^{ss}_c \tag{60}$$

$$q^{ss}_1 = \omega^{-1}(\beta \frac{z_m}{\gamma}) \tag{61}$$

$$q^{ss}_2 = \omega^{-1}(\beta z_c(1-\kappa)) \tag{62}$$

$$\Delta^{ss} = \kappa M^{ss}_c \tag{63}$$

Under Assumptions 2.1 and 2.2 and given the parameters of the model, there is a unique set of equilibrium outcomes that satisfy (58)-(63), so long as $\beta < \gamma < \bar{\gamma}$ and $0 < \bar{\mu}$, where $\bar{\gamma}$ and $\bar{\mu}$ are obtained from (47)-(48) with $\alpha_3 = 0$.

Similar to Proposition 5, since each currency is essential in some transactions, agents will hold both currencies to smooth consumption in two decentralized markets, so long as neither currency is too costly to carry. Thus, cryptocurrency and fiat money can coexist in the economy with different rates of return.

However, unlike the economy in which agents can trade with both currencies in a decentralized market, Proposition 6 shows that there is a dichotomy between two currencies' sectors in the economy with $\alpha_3 = 0$. In particular, the real values of cryptocurrency and fiat money are are independent, and the quantity of the DM good traded with cryptocurrency in DM2 is determined independently from that traded with fiat money in DM1. Moreover, the government monetary policy, γ, has no effects on the value and demand for cryptocurrency use, and the equilibrium outcomes of cryptocurrency only depend on the fundamentals of the economy, such as preferences, technologies, and trading frictions. Specifically, the real value of fiat money goes down as γ increases because fiat money becomes more costly to use and agents demand less for it, but the value of cryptocurrency is not affected in that case. Similarly for cryptocurrency: if it is lost at a higher rate or if its marginal production cost diminishes, the cost of carrying it increases, and thus the real value of cryptocurrency decreases, and that of fiat money remain unchanged.

6.2. Inherent Advantage to One Currency

I then consider a two-currency economy where one currency has an inherent advantage, modeled as degrees of acceptability in decentralized markets, relative to the other currency.

6.2.1. Inherent Advantage to Cryptocurrency

First, suppose there are only DM2 and DM3 in the economy, i.e., $\alpha_1 = 0,\ \alpha_2, \alpha_3 \in (0,1)$, and $\alpha_2 + \alpha_3 = 1$. In this set-up, cryptocurrency has an inherent advantage relative to fiat money because agents can trade with cryptocurrency everywhere but can only trade with fiat money in DM3. Then the equilibrium outcomes can be expressed as follows.

$$i_m \ \geq\ \alpha_3 \sigma L(\frac{z_m}{\gamma} + \frac{z_c(1-\kappa)}{1+\mu}) \qquad \text{“}=\text{”} \text{ if } \ z_m > 0 \tag{64}$$

$$i_c \ \geq\ \alpha_2 \sigma L(\frac{z_c(1-\kappa)}{1+\mu}) + \alpha_3 \sigma L(\frac{z_m}{\gamma} + \frac{z_c(1-\kappa)}{1+\mu}) \qquad \text{“}=\text{”} \text{ if } \ z_c > 0 \tag{65}$$

Agents compare the cost and benefit of holding the currency when they make currency portfolios choices. Under the condition that cryptocurrency can be used everywhere, the rate of return on fiat money has to be sufficiently higher than that on cryptocurrency in equilibrium with both currencies in circulation.

Proposition 7. *Given γ and $\{\alpha_1, \alpha_2, \alpha_3\}$ s.t. $\alpha_1 = 0,\ \alpha_2, \alpha_3 \in (0,1)$, and $\alpha_2 + \alpha_3 = 1$, under Assumptions 2.1 and 2.2, there exists a unique stationary equilibrium in which cryptocurrency and fiat money are valued in the economy, and in which the price of cryptocurrency is constant and that of fiat money changes at a constant rate s.t. $p^m_{t+1} = \frac{1}{\gamma} p^m_t$, so long as $\beta < \gamma < \bar{\gamma} \equiv \alpha_3(\frac{1}{1-\kappa} - \beta) + \beta$ and $0 < \hat{\mu} \equiv (\alpha_2 \sigma L(0) + 1)\beta(1-\kappa) - 1$. The equilibrium outcomes are characterized by:*

$$\frac{\gamma - \beta}{\sigma\beta} = \alpha_3 [\frac{u' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\kappa)))}{\omega' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\kappa)))} - 1] \tag{66}$$

$$\frac{1 - \beta(1-\kappa)}{\sigma\beta(1-\kappa)} = \alpha_2 [\frac{u' \circ \omega^{-1}(\beta z_c(1-\kappa))}{\omega' \circ \omega^{-1}(\beta z_c(1-\kappa))} - 1] + \frac{\gamma - \beta}{\sigma\beta} \tag{67}$$

$$f(p^{ss}_c, M^{ss}_c) = \kappa M^{ss}_c \tag{68}$$

$$q^{ss}_2 = \omega^{-1}(\beta z_c(1-\kappa)) \tag{69}$$

$$q^{ss}_3 = \omega^{-1}(\beta \frac{z_m}{\gamma} + \beta z_c(1-\kappa)) \tag{70}$$

$$\Delta^{ss} = \kappa M^{ss}_c \tag{71}$$

Since cryptocurrency can be used as a payment method everywhere, agents will carry it to facilitate all kinds of transactions in decentralized markets, as long as it is not too costly to hold. In order to give agents enough incentive to carry fiat money as well, the rate of return on fiat money has to be sufficiently high, or the inflation rate sufficiently low, in equilibrium with both currencies in circulation. Thus, there is a stationary equilibrium in which both currencies are valued, as long as fiat money is issued at a growth rate below a certain level, $\bar{\gamma}$, where $\bar{\gamma}$ depends on the fundamentals of cryptocurrency and the economy.

Moreover, the real value of cryptocurrency would increase if the cost of carrying it decreases (i.e., $\kappa \downarrow$ or $\frac{\partial c(\delta,M)}{\partial \delta} \uparrow$), or if the size of the market in which only cryptocurrency is accepted increases (i.e., $\alpha_2 \uparrow$). In these cases, agents would demand more for cryptocurrency and demand less for fiat money in decentralized meetings. Meanwhile, the parameter region $\bar{\gamma}$ gets lower under the above conditions, which means that fiat money has to be issued at a even lower growth rate in order to be valued in the economy. Otherwise, only cryptocurrency is valued and circulating in the economy.

6.2.2. Inherent Advantage to Fiat money

Symmetrically, suppose there are only DM1 and DM3 in the economy, i.e., $\alpha_2 = 0,\ \alpha_1, \alpha_3 \in (0,1)$, and $\alpha_1 + \alpha_3 = 1$. Then there is an inherent advantage to fiat money, since it is accepted everywhere, whereas cryptocurrency is only accepted in DM3. Then the equilibrium conditions (43)-(44) can be expressed as follows.

$$i_m \ \geq \ \alpha_1 \sigma L(\frac{z_m}{\gamma}) + \alpha_3 \sigma L(\frac{z_m}{\gamma} + \frac{z_c(1-\kappa)}{1+\mu}) \qquad \text{“} = \text{” if } \ z_m > 0 \tag{72}$$

$$i_c \ \geq \ \alpha_3 \sigma L(\frac{z_m}{\gamma} + \frac{z_c(1-\kappa)}{1+\mu}) \qquad \text{“} = \text{” if } \ z_c > 0 \tag{73}$$

Under the condition that fiat money is more acceptable, in order for cryptocurrency to be valued in the economy, the rate of return on cryptocurrency has to be sufficiently higher than that of fiat money in equilibrium.

Proposition 8. *Given γ and $\{\alpha_1, \alpha_2, \alpha_3\}$ s.t. $\alpha_2 = 0, \alpha_1, \alpha_3 \in (0,1)$, and $\alpha_1 + \alpha_3 = 1$, under Assumptions 2.1 and 2.2, there exists a unique stationary equilibrium in which both cryptocurrency and fiat money coexist in the economy, and in which the price of cryptocurrency is constant and that of fiat money changes at a constant rate s.t. $p^m_{t+1} = \frac{1}{\gamma} p^m_t$, so long as $\frac{1}{\alpha_3}(\frac{1}{1-\kappa} - \beta) + \beta \equiv \hat{\gamma} < \gamma < \bar{\gamma} \equiv \beta \alpha_1 \sigma L(0) + \frac{1}{1-\kappa}$. Gresham's law does not hold. The equilibrium outcomes are characterized by:*

$$\frac{\gamma-\beta}{\sigma\beta}=\alpha_1[\frac{u'\circ\omega^{-1}(\beta\frac{z_m}{\gamma})}{\omega'\circ\omega^{-1}(\beta\frac{z_m}{\gamma})}-1]+\frac{1-\beta(1-\kappa)}{\sigma\beta(1-\kappa)} \tag{74}$$

$$\frac{1-\beta(1-\kappa)}{\sigma\beta(1-\kappa)}=\alpha_3[\frac{u'\circ\omega^{-1}(\beta(\frac{z_m}{\gamma}+z_c(1-\kappa)))}{\omega'\circ\omega^{-1}(\beta(\frac{z_m}{\gamma}+z_c(1-\kappa)))}-1] \tag{75}$$

$$f(p_c^{ss},M_c^{ss})=\kappa M_c^{ss} \tag{76}$$

$$q_1^{ss}=\omega^{-1}(\beta\frac{z_m^{ss}}{\gamma}) \tag{77}$$

$$q_3^{ss}=\omega^{-1}(\beta\frac{z_m^{ss}}{\gamma}+\beta z_c(1-\kappa)) \tag{78}$$

$$\Delta^{ss}=\kappa M_c^{ss} \tag{79}$$

In this setting, agents will carry fiat money to facilitate all kinds of transactions in decentralized meetings, as long as it is not too costly to hold. Agents will carry cryptocurrency as well when the rate of return on it is much higher than that on fiat money e.g., fiat money is issued at a growth rate higher than a certain level, $\hat{\gamma}$, and thus, has a high inflation rate in equilibrium.

The parameter region $\hat{\gamma}$ gets higher when the cost of carrying cryptocurrency increases (i.e., $\kappa\uparrow$ or $\frac{\partial c(\delta,M)}{\partial\delta}\downarrow$) or when cryptocurrency becomes less acceptable (i.e., $\alpha_3\downarrow$). In these cases, agents demand more for fiat money, and cryptocurrency can coexist with fiat money even if fiat money is issued at a higher rate, as long as the new growth rate is below the new $\hat{\gamma}$.

Moreover, Proposition 8 shows that, Gresham's Law does not hold in this economy because both "bad" and "good" assets can circulate in equilibrium. Cryptocurrency, which is, in some sense, inferior in production costs and degrees of acceptability in decentralized markets, can coexist with fiat money, an asset that is more acceptable and costless to produce, when appropriate monetary policy is implemented. This result is different from previous work on fiat monies and commodity monies. For example, Velde et al. (1999) show that Gresham's Law holds in an economy with heavy and light coins, in the way that bad money is always traded while good money is traded if and only if the seller is informed. In contrast, the model proposed by Camera et al. (2004) produces the highest velocity for the good money, that is characterized by a purchasing power risk, in the way that agents favor spending the safe money and holding on to the risky one for subsequent trades, where Gresham's Law has been reversed.

Overall, in the economy of cryptocurrency and fiat money, when one currency has an inherent advantage as compared to the other, the rate of return on the less acceptable currency has to be higher in equilibrium with both currencies in circulation.

6.3. Implication

According to Propositions 5 – 8, the competition with cryptocurrency restricts the inflation rate of fiat money. Specifically, in the economy where cryptocurrency is more acceptable in decentralized markets, fiat money has to maintain sufficiently low inflation in order to be valued and circulating in equilibrium; while in the economy where fiat money is more acceptable, cryptocurrency will be valued as well when the inflation rate of fiat money is above a certain level. Therefore, the existence of cryptocurrency restricts the government's ability to raise its seigniorage by over-issuing fiat money.

Should the government ban cryptocurrency? It depends on the degree of acceptability of cryptocurrency in decentralized markets and whether the government can commit to maintaining the targeted fiat money growth rule. Because cryptocurrency is costly to produce, banning cryptocurrency will avoid the resource cost on production, i.e., $c(\delta, M^c)$. However, since agents in DM2 are only allowed to trade using cryptocurrency, banning cryptocurrency will result in welfare loss from no trade surplus in DM2, s.t. $-\alpha_2[u(q_2) - \omega(q_2)]$, where $q_2 = \omega^{-1}(\beta z_c(1-\kappa))$, and result in welfare changes from trade surplus in DM3 where both currencies are accepted, s.t. $\alpha_3[u(q_3^{'}) - \omega(q_3^{'})] - \alpha_3[u(q_3) - \omega(q_3)]$, where $q_3^{'} = \omega^{-1}(\beta\frac{z_m}{\gamma})$ and $q_3 = \omega^{-1}(\beta\frac{z_m}{\gamma} + \beta z_c(1-\kappa))$.

In addition, the competition with cryptocurrency restricts the government's ability to over-issue fiat money. If the government can maintain sufficiently low inflation and the market size of the DM2 is small, then banning cryptocurrency might be welfare-enhancing, because there would be no resource waste on producing cryptocurrency and agents could consume more DM goods using fiat money in decentralized markets, which would outweigh the welfare loss from no trade surplus in DM2.[27] Efficient allocations in DM1 and DM3 can be achieved when the monetary policy follows the Friedman rule if cryptocurrency is banned. However, if the government tends to over-issue money, banning cryptocurrency would worsen the welfare of the economy because there would be welfare loss in all decentralized markets: no trade surplus in DM2 and less trade surplus in DM1 and DM3 from consuming fewer DM goods using fiat money. Moreover, because a monetary equilibrium with cryptocurrency will deliver price stability and be consistent with zero inflation, the government that tends to use the inflation tax has a strong incentive to ban the use of cryptocurrency.

[27] All the trades with cryptocurrency in decentralized markets are assumed to be legitimate. For transactions that involve criminal activities, Camera (2001) introduces an external utility cost associated with the consumption of illegal goods and studies the governmental role in the presence of illegal activities. More recently, Hendrickson and Luther (2019) study the usage of cryptocurrencies to purchase illegal goods if the government is banning cash.

7. Conclusion

This paper studies the conditions under which cryptocurrency—a privately-issued money that is costly to produce—can be valued in equilibrium, and analyzes the conditions under which it can coexist with fiat money—an asset that is costless to produce—in search-theoretical models.

I first develop a model of monetary exchange in an economy with cryptocurrency only and incorporate profit-maximizing miners, who are able to produce cryptocurrency according to a costly technology. The production cost strictly increases in both the amount of newly produced units and the existing stock in circulation. Compared to fiat money economies—the inflation rate can be different from zero—and other types of private money economies—the inflation rate must necessarily be different from zero, the cryptocurrency economy has an advantage of being consistent with zero inflation, due to the shape of its production cost function.

I then extend my cryptocurrency-only model by adding fiat money and multiple decentralized markets to study the currency competition between cryptocurrency and fiat money. The two currencies differ in their supply rules, issuers, production costs, and degrees of acceptability in decentralized meetings. Different from the traditional two-fiat money models, in which rates of return on two currencies must be the same if both currencies are in circulation, cryptocurrency and fiat money can circulate regardless of their rates of return. Moreover, Gresham's Law does not hold in the sense that, even if cryptocurrency is inferior in production costs and acceptability in decentralized meetings, cryptocurrency can coexist with fiat money, which is an asset that is more acceptable and is costless to produce, when appropriate monetary policy is implemented. Further, as agents can trade with both currencies in some decentralized meetings and cryptocurrency is consistent with zero inflation in stationary equilibrium, the competition with cryptocurrency restricts the government's ability to over-issue fiat money. Therefore, banning cryptocurrency would worsen the welfare of the economy, if the government tends to use the inflation tax.

This paper analyzes the currency competition between cryptocurrency and fiat money under limited conditions. Many other features of cryptocurrency could be relevant topics for future research, such as the free entry and exit of miners and additional service fees to miners. In addition, it is worth investigating the impact of monetary and fiscal policies on the cryptocurrency market, e.g., tax on miners or cryptocurrency holders and policy to reduce the trading size of the market where cryptocurrency is used for illegal transactions.

References

D. Andolfatto. Incentive-feasible deflation. *Journal of Monetary Economics*, 60(4):383–390, May 2013.

L. Araujo and B. Camargo. Information, learning, and the stability of fiat money. *Journal of Monetary Economics*, 53(7):1571–1591, October 2006.

L. Araujo and B. Camargo. Endogenous supply of fiat money. *Journal of Economic Theory*, 142 (1):48–72, September 2008.

S. B. Aruoba, G. Rocheteau, and C. Waller. Bargaining and the value of money. *Journal of Monetary Economics*, 54(8):2636–2655, November 2007.

G. Camera. Money, search and costly matchmaking. *Macroeconomic Dynamics*, 4:289–323, 2000.

G. Camera. Dirty money. *Journal of Monetary Economics*, 47(2):377–415, 2001.

G. Camera, B. Crag, and C. Waller. Currency competition in a fundamental model of money. *Journal of International Economics*, 62(2):521–544, 2004.

V. Chari and C. Phelan. On the social usefulness of fractional reserve banking. *Journal of Monetary Economics*, 65:1–13, July 2014.

J. Chiu and T. V. Koeppl. The economics of cryptocurrencies-bitcoin and beyonds. *Bank of Canada Staff Working Paper 2019-40*, September 2019.

J. Chiu, M. Davoodalhosseini, J. Jiang, and Y. Zhu. Bank market power and central bank digital currency: Theory and quantitative assessment. *Working Paper*, June 2020.

M. Choi and G. Rocheteau. Money mining and price dynamics. *American Economic Journal: Macroeconomics (Forthcoming)*, 2020a.

M. Choi and G. Rocheteau. More on money mining and price dynamics: Competing and divisible currencies. *Working Paper*, 2020b.

B. Craig and C. Waller. Dual-currency economies as multiple-payment systems. *Federal Reserve Bank of Cleveland, Economic Review*, Q1, 2000.

E. S. Curtis and C. Waller. A search-theoretic model of legal and illegal currency. *Journal of Monetary Economics*, 45(1):155–184, February 2000.

M. Engineer. Currency transactions costs and competing fiat currencies. *Journal of International Economics*, 52(1):113–136, October 2000.

J. Fernández-Villaverde and D. Sanches. Cryptocurrencies: Some lessons from monetary economics. *Working Paper*, 2018.

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

F. A. V. Hayek. *Denationalization of Money: An Analysis of the Theory and Practice of Concurrent Currencies*. The Collected Works of F.A. Hayek, Good Money, Part 2,. The University of Chicago Press, 1999.

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

P. He, L. Huang, and R. Wright. Money, banking, and monetary policy. *Journal of Monetary Economics*, 55(6):1013–1024, September 2008.

J. R. Hendrickson and W. J. Luther. Cash, crime, and cryptocurrencies. *AIER Sound Money Project Working Paper 2019-01*, 2019.

T.-W. Hu and G. Rocheteau. On the coexistence of money and higher-return assets and its social role. *Journal of Economic Theory*, 148:2520–2560, 2013.

K. Iwasaki. In the indeterminacy of equilibrium exchange rates. *Working Paper*, 2020.

C. M. Kahn and W. Roberds. Credit and identity theft. *Journal of Monetary Economics*, 55: 251–264, 2008.

C. M. Kahn, F. Rivadeneyra, and T.-N. Wong. Eggs in one basket: Security and convenience of digital currencies. *Federal Reserve Bank of St. Louis Working Paper 2020-032*, 2020.

J. Kareken and N. Wallace. In the indeterminacy of equilibrium exchange rates. *The Quarterly Journal of Economics*, 96:207–222, May 1981.

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

N. Kiyotaki and R. Wright. A search-theoretic approach to monetary economics. *The American Economic Review*, 83(1):63–77, March 1993.

N. R. Kocherlakota. Money is memory. *Journal of Economic Theory*, 81(2):232–251, August 1998.

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

R. Lagos and R. Wright. Dynamics, cycles, and sunspot equilibria in 'genuinely dynamic, fundamentally disaggregative' models of money. *Journal of Economic Theory*, 109(2):156–171, April 2003.

R. Lagos and R. Wright. A unified framework for monetary theory and policy analysis. *Journal of Political Economy*, 113(3):463–484, June 2005.

R. Lagos, G. Rocheteau, and R. Wright. Liquidity: A new monetarist perspective. *Journal of Economic Literature*, 55(2):371–440, 2017.

Y. Li. Currency and checking deposits as means of payment. *Review of Economic Dynamics*, 14 (2):403–417, April 2011.

R. E. Lucas. Interest rates and currency prices in a two-country world. *Journal of Monetary Economics*, 10:335–359, 1982.

K. Matsuyama, N. Kiyotaki, and A. Matsui. Toward a theory of international currency. *Review of Economic Studies*, 60(2):283–307, April 1993.

E. Nosal and G. Rocheteau. *Money, Payments, and Liquidity*. The MIT Press, 2011.

W. Qiao and N. Wallace. Optimal provision of costly currency. *Working Paper*, 2020.

G. Rocheteau and R. Wright. Money in search equilibrium, in competitive equilibrium, and in competitive search equilibrium. *Econometrica*, 73:175–202, 2005.

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

S. Shi. Money and prices: A model of search and bargaining. *Journal of Economic Theory*, 67(2): 467–496, December 1995.

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

F. R. Velde, W. E. Weber, and R. Wright. A model of commodity money, with applications to Gresham's Law and the debasement puzzle. *Review of Dynamics*, 2(1):291–323, January 1999.

N. Wallace. Whither monetary economics? *International Economic Review*, 42(4):847–869, November 2001.

S. Williamson and R. Wright. New monetarist economics: Models. *Federal Reserve Bank of Minneapolis Staff Report 443*, April 2010.

Y. You and K. S. Rogoff. Redeemable platform currencies. *NBER Working Paper No. 26464*, November 2019.

C. Zhang. An information-based theory of international currency. *Journal of International Economics*, 93(2):286–301, July 2014.

R. Zhou. Currency exchange in a random search model. *The Review of Economic Studies*, 64(2): 289–310, April 1997.

S. Zhou. Anonymity, secondary demand, and the velocity of cryptocurrency. *Working Paper*, November 2020.

T. Zhu and N. Wallace. Fixed and flexible exchange-rates in two matching models: Non-equivalence results. *Working Paper*, 2020.

Y. Zhu and S. Hendry. A framework for analyzing monetary policy in an economy with e-money. *Bank of Canada Staff Working Paper 2019-1*, January 2019.

Appendix A. Proofs of Lemmas and Propositions

A.1. Cryptocurrency-Only Model

Lemmas 2.1–2.4 are similar to previous work and follow directly from the discussion in the text.

[Proof of Lemma 2.5]

Proof. From (3), a buyer's optimal cryptocurrency holdings satisfy:

$$-p_t + V_t^{'}(m_t^b) = 0 \tag{A.1}$$

Following Lemmas 2.1 and 2.2, the DM value function (5) can be rewritten as follows:

$$V_t^b(m_t^b) = \beta(p_{t+1}(1-\kappa)m_t^b + W_{t+1}^b(0)) + v_t(m_t^b),$$

$$\text{where} \quad v_t(m_t^b) = \begin{cases} \sigma[u(q^*) - \omega(q^*)] & if \quad m_t^b \geq m_t^* \\ \sigma[u(\hat{q}_t(m_t^b)) - \omega(\hat{q}_t(m_t^b)] & if \quad m_t^b < m_t^* \end{cases}$$

Then we obtain:

$$V'(m_t^b) = \begin{cases} \beta p_{t+1}(1-\kappa) & if \quad m_t^b \geq m_t^* \\ \beta p_{t+1}(1-\kappa) + \sigma\beta p_{t+1}(1-\kappa)[\frac{u'(\hat{q}_t(m_t^b))}{\omega'(\hat{q}_t(m_t^b))} - 1] & if \quad m_t^b < m_t^* \end{cases} \tag{A.2}$$

It is clear that $V'(m_t^b) > 0,\ \forall m^b < m_t^*$. Next, $V''(m_t^b),\ \forall m^b < m_t^*$, can be derived as follows.

$$\begin{aligned} V^{''}(m_t^b) &= \sigma\beta p_{t+1}(1-\kappa)\frac{\frac{u^{''}(\hat{q}_t(m_t^b))\omega'(\hat{q}_t(m_t^b))\beta p_{t+1}(1-\kappa)}{\omega'\circ\omega^{-1}(\beta p_{t+1}(1-\kappa)m_t^b)} - \frac{u'(\hat{q}_t(m_t^b))\omega^{''}(\hat{q}_t(m_t^b))\beta p_{t+1}(1-\kappa)}{\omega'\circ\omega^{-1}(\beta p_{t+1}(1-\kappa)m_t^b)}}{[\omega'(\hat{q}_t(m_t^b))]^2} \\ &= \sigma\beta p_{t+1}(1-\kappa)\frac{u^{''}(\hat{q}_t(m_t^b))\omega'(\hat{q}_t(m_t^b))\beta p_{t+1}(1-\kappa) - u'(\hat{q}_t(m_t^b))\omega^{''}(\hat{q}_t(m_t^b))\beta p_{t+1}(1-\kappa)}{[\omega'(\hat{q}_t(m_t^b))]^3} \\ &= \sigma\beta^2 p_{t+1}^2(1-\kappa)^2\frac{\underbrace{u^{''}(\hat{q}_t(m_t^b))\omega'(\hat{q}_t(m_t^b))}_{<0} - \underbrace{u'(\hat{q}_t(m_t^b))\omega^{''}(\hat{q}_t(m_t^b))}_{\geq 0}}{\underbrace{[\omega'(\hat{q}_t(m_t^b))]^3}_{>0}} \qquad \text{(Under Assumption 2.1)} \\ &< 0 \end{aligned}$$

Then $V'(m_t^b) > 0$ and $V''(m_t^b) < 0,\ \forall m_t^b < m_t^*$. Therefore, $V(m_t^b)$ is concave $\forall m_t^b < m_t^*$, and there is a unique $m_t^b < m_t^*$ solving the problem (A.1), which is expressed as (14) according to (A.2).

□

[Proof of Lemma 2.6]

Proof. Taking the F.O.C. of (16) with respect to $[\delta_t^i]$, we obtain $p_t = \frac{\partial c(\delta_t^i, M_{t-1})}{\partial \delta_t^i}$. Under Assumption 2.2, $\frac{\partial c(\delta_t^i, M_{t-1})}{\partial \delta_t^i}$ is increasing in δ_t^i and M_{t-1}, and there is a function $f(\cdot, \cdot)$ that implies $p_t = \frac{\partial c(\delta_t^i, M_{t-1})}{\partial \delta_t^i} \Longrightarrow \delta_t^i = f(M_{t-1}, p_t)$. Since δ_t^i cannot be negative, we have $\delta_t^i = \max[0, f(M_{t-1}, p_t)]$. □

[Proof of Proposition 1]

Proof. In stationary, $p_t M_t = p_{t+1} M_{t+1} = z^{ss}$. Then $\frac{M_{t+1}}{M_t} = \frac{p_t}{p_{t+1}} = 1$ and following the cryptocurrency law of motion, $\Delta^{ss} = \kappa M^{ss}$, $\forall t$. Combining it with the aggregate production (18), we obtain (20). Next, following Lemmas 2.4 and 2.5, the aggregate demand of cryptocurrency, M^d, satisfies:

$$\frac{1 - \beta(1-\kappa)}{\sigma\beta(1-\kappa)} = [\frac{u' \circ \omega^{-1}(\beta p^{ss}(1-\kappa)M^d)}{\omega' \circ \omega^{-1}(\beta p^{ss}(1-\kappa)M^d)} - 1] \tag{A.3}$$

Under Assumption 2.1, $\frac{u'(q)}{\omega'(q)}$ goes to infinity as q approaches zero and equals 1 when $q = q^*$, and thus, $\frac{u'(q_t)}{\omega'(q_t)}$ is decreasing in q_t for $q_t < q^*$. Therefore, given the functional forms and parameters of the model, there exists a unique value of p^{ss} and M^{ss} that satisfy both (A.3) and (20) with $M^{ss} = M^d$. Then there is a unique value of $z^{ss} = p^{ss} M^{ss}$ that solves (19), and following Lemma 2.2, there is a unique q^{ss} that solves (21). By construction, the above results constitute a unique stationary monetary equilibrium in which the price of cryptocurrency is constant.

□

[Proof of Proposition 2]

Proof. Suppose there exists a stationary equilibrium in which the price changes at a constant rate, s.t. $\frac{p_t}{p_{t+1}} = \frac{M_{t+1}}{M_t} = (1+\mu)$, where $\mu > -\kappa$ and $\mu \neq 0$. From (1) and (18), the aggregate production of cryptocurrency Δ_{t+1} satisfies $\Delta_{t+1} = f(p_{t+1}, M_t)$ and $\Delta_{t+1} = (\mu + \kappa) M_t$, which implies:

$$f(p_{t+1}, M_t) = (\mu + \kappa) M_t \tag{A.4}$$

Following Lemmas 2.4 and 2.5, the aggregate demand of cryptocurrency, M_t^d, satisfies:

$$1 + \mu = \beta(1-\kappa)\{1 + \sigma[\frac{u' \circ \omega^{-1}(\beta p_{t+1}(1-\kappa)M_t^d)}{\omega' \circ \omega^{-1}(\beta p_{t+1}(1-\kappa)M_t^d)} - 1]\} \tag{A.5}$$

Under Assumptions 2.1 and 2.2 and given parameters of the model, p_{t+1} and M_t can be pinned down by (A.4) and (A.5) with $M_t = M_t^d$. Thus, p_{t+1} and M_t do not change, which contradicts to the assumption that the price of cryptocurrency changes over time.

□

[Proof of Proposition 3]

See Appendix C.

[Proof of Proposition 4]

Proof. According to Lemma 2.5, in equilibrium, the relation between values of cryptocurrency p_t and p_{t+1} can be written as $p_t = g(p_{t+1})$, such as:

$$p_t = \beta(1-\kappa)p_{t+1}(1-\sigma) + \beta\sigma(1-\kappa)p_{t+1}[\frac{u^{'} \circ \omega^{-1}(\beta p_{t+1}(1-\kappa)M_t)}{\omega^{'} \circ \omega^{-1}(\beta p_{t+1}(1-\kappa)M_t)}] \tag{A.6}$$

Under Assumption 2.1, there exists a unique $p_t = g(p_{t+1}),\ \forall p_{t+1} \geq 0$. Clearly, A.6 goes through the steady state points $(0,0)$ and (p^{ss}, p^{ss}) where $p^{ss} > 0$. Next, following Lagos and Wright (2003), I show that in the space (p_t, p_{t+1}), the phase line representing RHS of the (A.6) intersects the 45° line from below, s.t. $g'(p^{ss} \mid_{p^{ss}=0}) > 1$ and $g'(p^{ss} \mid_{p^{ss}>0}) < 1$.

From the law of motion and the aggregate production for cryptocurrency, the aggregate stock M_t satisfies $M_t = M_{t-1} + \max[0, f(p_t, M_{t-1})]$. Using the Implicit Function Theorem, the implicit differentiation becomes:

$$\frac{\partial p_t}{\partial p_{t+1}} = \frac{\beta(1-\kappa)(1-\sigma) + \beta\sigma(1-\kappa)[\frac{u' \circ \omega^{-1}(\cdot)}{\omega' \circ \omega^{-1}(\cdot)}] + \beta^2\sigma(1-\kappa)^2 p_{t+1} M_t [\frac{\frac{u" \circ \omega^{-1}(\cdot)\omega' \circ \omega^{-1}(\cdot)}{\omega' \circ \omega^{-1}(\cdot)} - \frac{u' \circ \omega^{-1}(\cdot)\omega" \circ \omega^{-1}(\cdot)}{\omega' \circ \omega^{-1}(\cdot)}}{[\omega' \circ \omega^{-1}(\cdot)]^2}]}{1 - \beta^2\sigma(1-\kappa)^2 p_{t+1}^2 \frac{\partial M_t}{\partial p_t}[\frac{\frac{u" \circ \omega^{-1}(\cdot)\omega' \circ \omega^{-1}(\cdot)}{\omega' \circ \omega^{-1}(\cdot)} - \frac{u' \circ \omega^{-1}(\cdot)\omega" \circ \omega^{-1}(\cdot)}{\omega' \circ \omega^{-1}(\cdot)}}{[\omega' \circ \omega^{-1}(\cdot)]^2}]}$$

Under Assumptions 2.1 and 2.2, $\frac{\partial M_t}{\partial p_t} \geq 0$ and $[\frac{\frac{u" \circ \omega^{-1}(\cdot)\omega' \circ \omega^{-1}(\cdot)}{\omega' \circ \omega^{-1}(\cdot)} - \frac{u' \circ \omega^{-1}(\cdot)\omega" \circ \omega^{-1}(\cdot)}{\omega' \circ \omega^{-1}(\cdot)}}{[\omega' \circ \omega^{-1}(\cdot)]^2}] < 0$. At the steady state points, we have:

$$\frac{\partial p_t}{\partial p_{t+1}} \mid_{p^{ss}=0} = \beta(1-\kappa)(1-\sigma) + \beta\sigma(1-\kappa)[\frac{u'(0)}{\omega'(0)}] \quad > 1$$

$$\frac{\partial p_t}{\partial p_{t+1}} \mid_{p^{ss}>0} = \frac{1 + \beta^2\sigma(1-\kappa)^2 p^{ss} M^{ss} \frac{u"(q^{ss})\omega'(q^{ss}) - u'(q^{ss})\omega"(q^{ss})}{[\omega'(q^{ss})]^3}}{1 - \beta^2\sigma(1-\kappa)^2 p^{ss^2} \frac{\partial M^{ss}}{\partial p^{ss}} \frac{u"(q^{ss})\omega'(q^{ss}) - u'(q^{ss})\omega"(q^{ss})}{[\omega'(q^{ss})]^3}} \quad < 1$$

As $g'(0) > 1$ and $g'(p^{ss}) < 1, \forall p_0 < p^{ss}$, there exists a continuum of equilibria converging to the non-monetary equilibrium.

□

A.2. ***No Production of Cryptocurrency***

This section provides a special case to the stationary monetary equilibrium of a cryptocurrency-only economy with no cryptocurrency production.

Proposition A.1. *Under Assumption 2.1, there exists a unique stationary monetary equilibrium in which the price of cryptocurrency changes at a constant rate s.t.* $p_{t+1} = \frac{1}{1-\kappa} p_t$*, and in which no cryptocurrency is produced. The equilibrium outcomes are characterized by:*

$$\frac{1-\beta}{\sigma\beta} = [\frac{u' \circ \omega^{-1}(\beta z^{ss})}{\omega' \circ \omega^{-1}(\beta z^{ss})} - 1] \tag{A.7}$$

$$q^{ss} = \omega^{-1}(\beta z^{ss}) \tag{A.8}$$

[Proof of Proposition A.1]

Proof. In stationary, the real balances of cryptocurrency are constant, then $\frac{M_{t+1}}{M_t} = \frac{p_t}{p_{t+1}} = 1-\kappa$ and $\Delta_t = 0 \ \forall t$. Following Lemmas 2.4 and 2.5, the real balance z^{ss} satisfies (A.7). Under Assumption 2.1, there exists a unique $z^{ss} > 0$ that solves (A.7). Next, following Lemma 2.2, the consumption of the DM good $q^{ss} < q^*$ can be uniquely determined by (A.8). By construction, the above results constitute a unique stationary monetary equilibrium in which the price of cryptocurrency changes at a constant rate. In that equilibrium, there is no production of new cryptocurrency, and the stock of cryptocurrency that circulates in the economy is the existing stock and subject to currency depreciation.

□

A.3. **Two-Currency Model**

Lemma 4.2 follows directly from the discussion in the text.

[Proof of Lemma 4.1]

Proof. Solutions to the terms of trade in each decentralized market follow from the discussion in the text, and $q_t^{DM}, DM \in \{1,2,3\}$, can be proved following Lemma 2.3.

i. $\forall\ m_t^{m,b} < m_t^{m*}, \quad \hat{q}_t^1(m_t^{m,b}) = \omega^{-1}(\beta p_{t+1}^m m_t^{m,b}) \ \Rightarrow \ \frac{\partial \hat{q}_t^1(m_t^{m,b})}{\partial m_t^{m,b}} = \frac{\beta p_{t+1}^m}{\omega'(\hat{q}_t^1(m_t^{m,b}))} > 0$

ii. $\forall\ m_t^{c,b} < m_t^{c*}, \quad \hat{q}_t^2(m_t^{c,b}) = \omega^{-1}(\beta p_{t+1}^c (1-\kappa) m_t^{c,b}) \ \Rightarrow \ \frac{\partial \hat{q}_t^2(m_t^{c,b})}{\partial m_t^{c,b}} = \frac{\beta p_{t+1}^c (1-\kappa)}{\omega'(\hat{q}_t^2(m_t^{c,b}))} > 0$

iii. $\forall\ \beta(p^m_{t+1}m^{m,b}_t + (1-\kappa)p^c_{t+1}m^{c,b}_t) < \omega(q^*), \quad \omega(\hat{q}^3_t(\mathbf{m}^b_t)) = \beta(p^m_{t+1}m^{m,b}_t + (1-\kappa)p^c_{t+1}m^{c,b}_t)$

$$\Rightarrow \frac{\partial \hat{q}^3_t(\mathbf{m}^b_t)}{\partial m^{m,b}_t} = \frac{\beta p^m_{t+1}}{\omega'(\hat{q}^3_t(\mathbf{m}^b_t))} > 0 \quad \text{and} \quad \frac{\partial \hat{q}^3_t(\mathbf{m}^b_t)}{\partial m^{c,b}_t} = \frac{\beta p^c_{t+1}(1-\kappa)}{\omega'(\hat{q}^3_t(\mathbf{m}^b_t))} > 0$$

From Lemma 2.1, $\frac{\partial \hat{q}^1_t(m^{m,b}_t)}{\partial m^{m,b}_t}, \frac{\partial \hat{q}^1_2(m^{c,b}_t)}{\partial m^{c,b}_t}, \frac{\partial \hat{q}^3_t(\mathbf{m}^b_t)}{\partial m^{m,b}_t}, \frac{\partial \hat{q}^3_t(\mathbf{m}^b_t)}{\partial m^{c,b}_t} > 0$, and $\hat{q}^1_t, \hat{q}^2_t, \hat{q}^3_t < q^*$.

□

[Proof of Proposition 5]

Proof. In stationary, $p^k_t M^k_t = p^k_{t+1}M^k_{t+1} = z^{ss}_k, k \in \{m, c\}$. From Propositions 1 and 2, the price of cryptocurrency must remain constant in a stationary monetary equilibrium. When $M^m_{t+1} = \gamma M^m_t$ and $M^c_{t+1} = M^c_t$, a stationary equilibrium in which $z_m > 0$ and $z_c > 0$ exists, so long as $\beta < \gamma < \bar{\gamma}$ and $0 < \hat{\mu}$, where $\bar{\gamma} = \beta\alpha_1\sigma L(0) + \frac{\alpha_3}{\alpha_2+\alpha_3}(\frac{1}{1-\kappa} - \beta) + \beta$ is obtained from (48) by replacing $\mu = 0$, and $\hat{\mu} = \beta(1-\kappa)\{\alpha_2\sigma L(0) + 1\} - 1$ is obtained from (47), given $\gamma \in (\beta, \bar{\gamma})$.

From (1) and (18), the aggregate production of cryptocurrency satisfies $\Delta^{ss} = f(p^{ss}_c, M^{ss}_c)$ and $\Delta^{ss} = \kappa M^{ss}_c$, which implies (51). From (43)-(44), the real balances of the two currencies, z^{ss}_m and $z^{ss}_c = p^{ss}_c M^{ss}_c$, satisfy (49)-(50). Following Lemma 4.1, the steady state consumption of the DM good in each decentralized market satisfies (52)-(54). Given the functional forms and parameters of the model, the equilibrium outcomes can be jointly determined by (49)-(55), under Assumptions 2.1 and 2.2. By construction, the above results constitute a stationary equilibrium in which both currencies are valued.

□

[Proof of Proposition 6]

Proof. Everything follows the Proof of Proposition 5 by replacing $\alpha_3 = 0$. Then, under Assumptions 2.1 and 2.2, a set of equilibrium outcomes can be uniquely determined using (58)-(63), given the functional forms and parameters of the model.

□

[Proof of Proposition 7]

Proof. Everything follows the Proof of Proposition 5 by replacing $\alpha_1 = 0$. The parameter region $\bar{\gamma}$ is obtained from (48) with $\alpha_1 = \mu = 0$, and $\hat{\mu}$ is obtained from (47) given $\gamma \in (\beta, \bar{\gamma})$. Similarly, the equilibrium outcomes can be uniquely determined by (66)-(71), given the functional forms $u(\cdot), \omega(\cdot)$, and model parameters, under Assumptions 2.1 and 2.2.

□

[Proof of Proposition 8]

Proof. In stationary, the real balance of each currency is constant. When $M^m_{t+1} = \gamma M^m_t$ and $M^c_{t+1} = M^c_t$, a stationary equilibrium in which $z_m > 0$ and $z_c > 0$ exists, so long as $\hat{\gamma} \leq \gamma < \bar{\gamma}$, where $\bar{\gamma} = \beta\alpha_1\sigma L(0) + \frac{1}{1-\kappa}$ is obtained from (48) with $\mu = \alpha_2 = 0$ and $\hat{\gamma} = \frac{1}{\alpha_3}(\frac{1}{1-\kappa} - \beta) + \beta$ is obtained from (47) with $\bar{\mu} > 0$. Then, following the Proof of Proposition 5 by replacing $\alpha_2 = 0$, there exists a unique set of equilibrium outcomes that satisfy (74)-(79), under Assumptions 2.1 and 2.2, and given fundamentals of the model.

□

Appendix B. An Extension of Cryptocurrency Security

In this section, I alternatively model the cryptocurrency security in the cryptocurrency-only economy as theft instead of loss in the main text. The difference between loss and theft is that loss means a fraction of cryptocurrency holdings is gone for every agent. In contrast, theft means some agents lose a fraction of their cryptocurrency holdings, but other agents get those lost units, making the aggregate stock of cryptocurrency unchanged before the new production. Then the new cryptocurrency law of motion becomes:

$$M_t = M_{t-1} + \Delta_t \tag{B.1}$$

I show that similar to the model with currency loss, there is no stationary monetary equilibrium in which the price of cryptocurrency changes over time. However, different from the model with currency loss, in this economy, there is no production of cryptocurrency in a stationary monetary equilibrium. That is, the cryptocurrency production will stop, and the only units that circulate in the economy will be the existing stuff.

B.1. Buyers and Sellers

In the first sub-period, a typical buyer b and seller s enter the centralized market with m^b_{t-1} and m^s_{t-1} units of cryptocurrency from the last period, respectively. In the centralized market, a fraction of the buyer's cryptocurrency holdings, κm^b_{t-1}, is thieved, and meanwhile, the seller gets these thieved cryptocurrency units. Then the CM value functions become:

$$W^b_t(m^b_{t-1}) = \max_{x^b_t, m^b_t} \quad x^b_t + V^b_t(m^b_t), \qquad s.t. \qquad x^b_t + p_t m^b_t = p_t(1-\kappa)m^b_{t-1}$$

$$W^s_t(m^s_{t-1}) = \max_{x^s_t, m^s_t} \quad x^s_t + V^s_t(m^s_t), \qquad s.t. \qquad x^s_t + p_t m^s_t = p_t(m^s_{t-1} + \kappa m^b_{t-1})$$

The above CM value functions can be rearranged as:

$$W_t^b(m_{t-1}^b) = p_t(1-\kappa)m_{t-1}^b + \underbrace{\max_{m_t^b \in \mathbb{R}_+} -p_t m_t^b + V_t^b(m_t^b)}_{W_t^b(0)} \tag{B.2}$$

$$W_t^s(m_{t-1}^s) = p_t(m_{t-1}^s + \kappa m_{t-1}^b) + \underbrace{\max_{m_t^s \in \mathbb{R}_+} -p_t m_t^s + V_t^s(m_t^s)}_{W_t^s(0)} \tag{B.3}$$

Similar to Lemma 2.1, the choices of cryptocurrency holdings are independent of the agent's initial cryptocurrency holdings when entering the centralized market, cryptocurrency losses, and theft.

In the second sub-period, the buyer and seller enter the decentralized market with m_t^b and m_t^s units of cryptocurrency, respectively. The DM value functions are the same as (5)-(6).

According to (B.2)-(B.3), the terms of trade are given by the solution to:

$$\begin{aligned} \max_{q_t, d_t} \quad & u(q_t) - \beta p_{t+1}(1-\kappa)d_t \\ s.t. \quad & -\omega(q_t) + \beta p_{t+1} d_t \geq 0 \\ & d_t \leq m_t^b \end{aligned} \tag{B.4}$$

Lemma B.1. *The terms of trade, (q_t, d_t), that solve problem (B.4) are given by:*

$$q_t(m_t^b) = \begin{cases} q^* & if \quad m_t^b \geq m_t^* \\ \hat{q}_t & if \quad m_t^b < m_t^* \end{cases} \qquad d_t(m_t^b) = \begin{cases} m_t^* & if \quad m_t^b \geq m_t^* \\ m_t^b & if \quad m_t^b < m_t^* \end{cases} \tag{B.5}$$

where $q^* = argmax\,[u(q_t) - (1-\kappa)\omega(q_t)]$, $m_t^* = \frac{\omega(q^*)}{\beta p_{t+1}}$, and $\hat{q}_t = \omega^{-1}(\beta p_{t+1} m_t^b)$.

Then the DM value functions can be expressed as:

$$V_t^b(m_t^b) = \beta(p_{t+1}(1-\kappa)m_t^b + W_{t+1}^b(0)) + \sigma[u(q_t(m_t^b)) - (1-\kappa)\omega(q_t(m_t^b))] \tag{B.6}$$

$$V_t^s(m_t^s) = \beta(p_{t+1}(m_t^s + \kappa m_t^b) + W_{t+1}^s(0)) + 0 \tag{B.7}$$

Next, from (B.2)-(B.3), the optimal cryptocurrency holdings of a buyer and seller are given by the solutions to:

$$W_t^b(m_{t-1}^b) = \max_{m_t^b \in \mathbb{R}_+} -(p_t - p_{t+1}\beta(1-\kappa))m_t^b + \sigma[u(q_t(m_t^b)) - (1-\kappa)\omega(q_t(m_t^b))] \tag{B.8}$$

$$W_t^s(m_{t-1}^s) = \max_{m_t^s \in \mathbb{R}_+} -(p_t - p_{t+1}\beta)m_t^s + 0 \tag{B.9}$$

The optimal cryptocurrency holdings of a typical buyer and seller satisfy:

$$-p_t + \beta p_{t+1}(1-\kappa) + v_t^{'}(m_t^b) \leq 0 \qquad \text{“}=\text{”} \text{ if } \quad m_t^b > 0 \tag{B.10}$$

$$-p_t + \beta p_{t+1} \leq 0 \qquad \text{“}=\text{”} \text{ if } \quad m_t^s > 0 \tag{B.11}$$

$$\text{where } v_t^{'}(m_t^b) = \begin{cases} 0 & \text{if} \quad m_t^b \geq m_t^* \\ \sigma\beta p_{t+1}[\frac{u'(\hat{q}_t(m_t^b))}{\omega'(\hat{q}_t(m_t^b))} - (1-\kappa)] > 0 & \text{if} \quad m_t^b < m_t^* \end{cases}$$

When cryptocurrency is costly to carry for buyers, i.e., $\frac{p_t}{p_{t+1}} > \beta(1-\kappa)$, they will only carry what they expect to spend in the decentralized meeting.

B.2. ***Miners***

The miner's problem is the same as in the cryptocurrency-only model with cryptocurrency loss. So the aggregate new cryptocurrency supplied in period t, Δ_t, satisfies (18).

B.3. **Stationary Equilibrium**

The equilibrium definitions are the same as in Section 3, except for cryptocurrency law of motion.

Proposition B.1. *Under Assumption 2.1, there exists a unique stationary monetary equilibrium, in which the price of cryptocurrency is constant. The equilibrium outcomes are characterized by:*

$$\frac{1-\beta(1-\kappa)}{\sigma\beta} = [\frac{u' \circ \omega^{-1}(\beta z^{ss})}{\omega' \circ \omega^{-1}(\beta z^{ss})} - (1-\kappa)] \tag{B.12}$$

$$q^{ss} = \omega^{-1}(\beta z^{ss}) \tag{B.13}$$

$$\Delta = 0 \tag{B.14}$$

[Proof of Proposition B.1]

Proof. In stationary, $p_t M_t = p_{t+1} M_{t+1} = z^{ss}$, $\forall t$. Following (B.1), $\Delta_t = 0$. Then following the optimal cryptocurrency holdings conditions and market clearing for cryptocurrency, the real balance z^{ss} satisfies (B.12). Under Assumption 2.1, there exists a unique z^{ss} solving (B.12). Then following Lemma B.1, the steady state consumption of the DM good, $q^{ss} < q^*$, is uniquely determined by (B.13). By construction, the above results constitute a unique stationary monetary equilibrium, in

which the price of cryptocurrency is constant. In this equilibrium, no cryptocurrency is produced. □

Proposition B.2. *Under Assumptions 2.1 and 2.2, there does not exist a stationary monetary equilibrium in which the price changes at a constant rate s.t.* $\frac{p_t}{p_{t+1}} = (1+\mu), \mu \neq 0$.

[Proof of Proposition B.2]

Proof. Suppose there is a set of variables that construct a stationary equilibrium with the price changes at a constant rate s.t. $\frac{p_t}{p_{t+1}} = \frac{M_{t+1}}{M_t} = (1+\mu)$. From (B.1) and (18), the aggregate production of cryptocurrency satisfies $\Delta_{t+1} = f(p_{t+1}, M_t)$ and $\Delta_{t+1} = \mu M_t$. Combining these two conditions, we obtain:

$$f(p_{t+1}, M_t) = \mu M_t \tag{B.15}$$

From (B.10), the aggregate demand of cryptocurrency, M_t^d, satisfies:

$$\frac{(1+\mu) - \beta(1-\kappa)(1-\sigma)}{\beta\sigma} = [\frac{u^{'} \circ \omega^{-1}(\beta p_{t+1} M_t^d)}{\omega^{'} \circ \omega^{-1}(\beta p_{t+1} M_t^d)}] \tag{B.16}$$

Under Assumptions 2.1 and 2.2, and given the parameters of the economy, p_{t+1} and M_t can be pinned down by (B.15) and (B.16) with $M_t = M_t^d$. Thus, p_{t+1} and M_t do not change, which contradicts to the assumption that the price of cryptocurrency changes over time.

□

Appendix C. Alternative Private Money Economy

In this section, I consider a private money economy in which the marginal cost of producing money is independent of the existing stock in circulation and in which the currency depreciation rate is zero.

Suppose the cost function of producing cryptocurrency is only convex in the newly produced units, as shows in Assumption 3.1. Then the maximization problem of a typical miner becomes:

$$\begin{aligned} \max_{x_t^i, \delta_t^i} \quad & \sum_{t=0}^{\infty} \beta^t x_t^i \\ \text{s.t.} \quad & x_t^i \leq p_t \delta_t^i - c(\delta_t^i) \quad \forall t \\ & x_t^i, \delta_t^i \geq 0 \qquad \forall t \end{aligned} \tag{C.1}$$

Given (C.1), the miner's problem in period t can be written as follows.

$$\max_{\delta_t^i \geq 0} \quad p_t \delta_t^i - c(\delta_t^i) \tag{C.2}$$

Lemma C.1. *Under Assumption 3.1, a typical miner i produces δ_t^i units of cryptocurrency in period t, given p_t and M_{t-1}, such that:*

$$\delta_t^i = \max[0, F(p_t)] \tag{C.3}$$

where $F(p_t)$ results from the F.O.C. of (C.2) with respect to δ_t^i, $p_t = \frac{\partial c(\delta_t^i)}{\partial \delta_t^i}$, which can be rewritten as $\delta_t^i = F(p_t)$.

Example C.1. *Suppose the production cost function takes the functional form: $c(\delta_t^i) = B{\delta_t^i}^2,\ B > 0$. In this case, a miner i would produce $\delta_t^i = \max[0, \frac{p_t}{2B}]$ units of cryptocurrency.*

From (C.3), the number of newly produced cryptocurrency in each period depends only on the value of cryptocurrency. Further, the aggregate new cryptocurrency in period t, Δ_t, becomes:

$$\Delta_t = \int_0^1 \delta_t^i di = \max[0, F(p_t)] \tag{C.4}$$

Suppose the currency depreciation rate is zero, i.e., $\kappa = 0$. As Proposition 3 states, a stationary monetary equilibrium of private money will not deliver price stability in an environment with $\kappa = 0$ and with the production cost function satisfying Assumption 3.1.

[Proof of Proposition 3]

Proof. Suppose there is a stationary equilibrium with $p_t = p_{t+1} = p^{ss} > 0$. Under Assumption 3.1 and given (C.4), $\Delta_t = F(p^{ss}) > 0$ and thus, $M_{t+1} > M_t$, which would eventually violate the transversality condition under price stability. Therefore, the price of cryptocurrency cannot maintain constant, and thus, the monetary equilibrium necessarily has positive inflation.

□

Appendix D. Exogenously Supplied Cryptocurrency

In this section, I develop a two-currency economy where the new cryptocurrency is exogenously supplied rather than endogenously produced. Specifically, there are no miners in the economy, and the aggregate new cryptocurrency in period t satisfies $\Delta_t = \epsilon M^c_{t-1}, \epsilon > 0$. The new cryptocurrency is implemented through lump-sum transfers to agents in the centralized market. Then the new cryptocurrency law of motion follows:

$$M^c_t = M^c_{t-1} + \Delta_t - \kappa M^c_{t-1} = (1 + \epsilon - \kappa) M^c_{t-1} \tag{D.1}$$

I show that there exists a stationary equilibrium in which both currencies are valued and in which the price of cryptocurrency changes at a constant rate. Therefore, different from the two-currency model with endogenously produced cryptocurrency in the main text, a two-currency model with exogenously supplied cryptocurrency cannot have an equilibrium in which the price of cryptocurrency must remain constant.

D.1. ***Buyers and Sellers***

The problems faced by a typical buyer and seller are the same as those in the two-currency economy described in Section 4, except for agents receiving the new cryptocurrency supply in the form of lump-sum transfers during the first sub-period, i.e., $T^c_t = p^c_t \epsilon M^c_{t-1}$, expressed in terms of the CM good. Thus, the CM value functions of a buyer and seller are:

$$W^b_t(\mathbf{m^b_{t-1}}) = p^m_t m^{m,b}_{t-1} + (1-\kappa) p^c_t m^{c,b}_{t-1} \underbrace{+ T^m_t + T^c_t + \max_{\mathbf{m^b_t} \in \mathbb{R}^2_+} -\mathbf{p_t m^b_t} + V^b_t(\mathbf{m^b_t})}_{W^b_t(0,0)} \tag{D.2}$$

$$W^s_t(\mathbf{m^s_{t-1}}) = p^m_t m^{m,s}_{t-1} + (1-\kappa) p^c_t m^{c,s}_{t-1} \underbrace{+ T^c_t + \max_{\mathbf{m^s_t} \in \mathbb{R}^2_+} -\mathbf{p_t m^s_t} + V^s_t(\mathbf{m^s_t})}_{W^s_t(0,0)} \tag{D.3}$$

From (D.2)-(D.3), an agent's choice of currency portfolio is independent of lump-sum transfers/taxes, cryptocurrency losses, and the agent's initial currency portfolio when entering the centralized market.

D.2. **Equilibrium**

Definition D.1. *Given γ and ϵ, an equilibrium is a set of decision rules in the centralized market $\{x^b_t, \mathbf{m}^b_t, x^s_t, \mathbf{m}^s_t\}^\infty_{t=0}$, the terms of trade in each decentralized market $\{(q^1_t, d^{1,m}_t), (q^2_t, d^{2,c}_t), (q^3_t, d^{3,m}_t,$*

$d_t^{3,c})\}_{t=0}^{\infty}$, *and sequences of values of cryptocurrency and fiat money* $\{p_t^c, p_t^m\}_{t=0}^{\infty}$, *such that for all* $t \geq 0$*:* $\{x_t^b, \mathbf{m}_t^b, x_t^s, \mathbf{m}_t^s\}$ *solve problems (D.2)-(D.3) and (29)-(30);* $\{(q_t^1, d_t^{1,m}), (q_t^2, d_t^{2,c}), (q_t^3, d_t^{3,m}, d_t^{3,c})\}$ *solve problems (34)-(36); as well as market clearing for centralized good, fiat money, and cryptocurrency, and the cryptocurrency law of motion and transversality conditions are satisfied.*

Next, I characterize the stationary equilibrium in which both currencies are valued, i.e., $z_m > 0$ and $z_c > 0$. Given $M_{t+1}^m = \gamma M_t^m$ where $\gamma > \beta$ and $M_{t+1}^c = (1+\epsilon-\kappa)M_t^c$ where $1+\epsilon-\kappa > \beta(1-\kappa)$, according to (43)-(44), the equilibrium conditions satisfy:

$$i_m \geq \alpha_1 \sigma L(\frac{z_m}{\gamma}) + \alpha_3 \sigma L(\frac{z_m}{\gamma} + \frac{(1-\kappa)z_c}{1+\epsilon-\kappa}) \qquad \text{“}=\text{”} \text{ if } z_m > 0 \tag{D.4}$$

$$i_c \geq \alpha_2 \sigma L(\frac{(1-\kappa)z_c}{1+\epsilon-\kappa}) + \alpha_3 \sigma L(\frac{z_m}{\gamma} + \frac{(1-\kappa)z_c}{1+\epsilon-\kappa}) \qquad \text{“}=\text{”} \text{ if } z_c > 0 \tag{D.5}$$

where $i_m = \frac{p_t^m}{\beta p_{t+1}^m} - 1$ and $i_c = \frac{p_t^c}{\beta p_{t+1}^c (1-\kappa)} - 1$. Following the existence conditions described in Section 5, cryptocurrency and fiat money can coexist so long as $\beta < \gamma < \bar{\gamma}$ and $\beta(1-\kappa) < 1+\epsilon-\kappa < 1+\bar{\mu}$, where $\bar{\gamma}$ and $\bar{\mu}$ are given by:

$$\frac{1+\bar{\mu}}{\beta(1-\kappa)} - 1 = \alpha_2 \sigma L(0) + \frac{\alpha_3}{\alpha_1+\alpha_3}(\frac{\gamma}{\beta} - 1) \tag{D.6}$$

$$\frac{\bar{\gamma}}{\beta} - 1 = \alpha_1 \sigma L(0) + \frac{\alpha_3}{\alpha_2+\alpha_3}(\frac{1+\epsilon-\kappa}{\beta(1-\kappa)} - 1) \tag{D.7}$$

D.3. Coexistence

Proposition D.1. *Given* γ, ϵ *and* $\alpha_{DM} \in (0,1)\ \forall DM \in \{1,2,3\}$*, under Assumption 2.1, there exists a stationary equilibrium in which both cryptocurrency and fiat money are valued, so long as* $\beta < \gamma < \bar{\gamma}$ *and* $\beta(1-\kappa) < 1+\epsilon-\kappa < 1+\bar{\mu}$*. The equilibrium outcomes are characterized by:*

$$\frac{\gamma-\beta}{\sigma\beta} = \alpha_1[\frac{u' \circ \omega^{-1}(\beta\frac{z_m}{\gamma})}{\omega' \circ \omega^{-1}(\beta\frac{z_m}{\gamma})} - 1] + \alpha_3[\frac{u' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + \frac{z_c(1-\kappa)}{1+\epsilon-\kappa}))}{\omega' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + \frac{z_c(1-\kappa)}{1+\epsilon-\kappa}))} - 1] \tag{D.8}$$

$$\frac{(1+\epsilon-\kappa)-\beta(1-\kappa)}{\sigma\beta(1-\kappa)} = \alpha_2[\frac{u' \circ \omega^{-1}(\beta\frac{z_c(1-\kappa)}{1+\epsilon-\kappa})}{\omega' \circ \omega^{-1}(\beta\frac{z_c(1-\kappa)}{1+\epsilon-\kappa})} - 1] + \alpha_3[\frac{u' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + \frac{z_c(1-\kappa)}{1+\epsilon-\kappa}))}{\omega' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + \frac{z_c(1-\kappa)}{1+\epsilon-\kappa}))} - 1] \tag{D.9}$$

$$q_1^{ss} = \omega^{-1}(\beta\frac{z_m}{\gamma}) \tag{D.10}$$

$$q_2^{ss} = \omega^{-1}(\beta\frac{z_c(1-\kappa)}{1+\epsilon-\kappa}) \tag{D.11}$$

$$q_3^{ss} = \omega^{-1}(\beta\frac{z_m}{\gamma} + \beta\frac{z_c(1-\kappa)}{1+\epsilon-\kappa}) \tag{D.12}$$

[Proof of Proposition D.1]

Proof. In stationary, $p_t^k M_t^k = p_{t+1}^k M_{t+1}^k = z_k^{ss}, \ \forall t, \ k \in \{m, c\}$. Given $\beta < \gamma < \bar{\gamma}$ and $\beta(1-\kappa) < 1 + \epsilon - \kappa < 1 + \bar{\mu}$, from (D.4)-(D.5), the real balances of the two currencies, z_m and z_c, satisfy (D.8)-(D.9). Following Lemma 4.1, the steady state consumption of the DM good in each decentralized market satisfies (D.10)-(D.12). Given the functional forms $u(\cdot), \omega(\cdot)$, and parameters of the model, a set of equilibrium outcomes can be jointly determined by (D.8)-(D.12), under Assumption 2.1. By construction, the above results constitute a stationary equilibrium, in which both fiat money and cryptocurrency are valued in the economy, where the supplies of cryptocurrency and fiat money grow at constant rates.

□

Appendix E. Miners Carry Currencies

In this section, I alternatively assume that miners are allowed to carry currencies in the economy.

E.1. Carry Cryptocurrency

First, I describe the problem of miners in the cryptocurrency-only economy. I show that when miners are allowed to carry cryptocurrency, they will sell all the newly produced cryptocurrency after the production in equilibrium.

In the centralized market, a typical miner i chooses the consumption of the CM good, x_t^i, the amount of new cryptocurrency to produce, δ_t^i, and cryptocurrency holdings, m_t^i. Since miners remain idle in the second sub-period, the maximization problem of a typical miner is represented by:

$$W_t(m_{t-1}^i) = \max_{\delta_t^i, m_t^i} \quad p_t \delta_t^i - c(\delta_t^i, M_{t-1}) + p_t(1-\kappa) m_{t-1}^i - p_t m_t^i + \beta W_{t+1}(m_t^i) \tag{E.1}$$

Taking the F.O.C. with respect to δ_t^i and m_t^i, we have:

$$p_t = \frac{\partial c(\delta_t^i, M_{t-1})}{\partial \delta_t^i} \tag{E.2}$$

$$-p_t + \beta p_{t+1}(1-\kappa) \leq 0 \qquad \text{“}=\text{”} \quad \text{if} \quad m_t^i > 0 \tag{E.3}$$

From (E.2), a miner will produce $\delta_t^i = \max\,[\,0, f(p_t, M_{t-1})]$ units of cryptocurrency in period t. From (E.3), a miner will not hold any newly produced cryptocurrency when $p_t > \beta p_{t+1}(1-\kappa)$. Since miners do not participate in the second sub-period, they do not have an incentive to carry

cryptocurrency out of the centralized market. Therefore, in a stationary monetary equilibrium in which the price of cryptocurrency is stable, miners do not keep any newly produced cryptocurrencies, $m_t^i = 0,\ \forall t$.

E.2. Carry Fiat Money

Next, I describe the problem of miners in the two-currency economy in which miners are allowed to carry fiat money.

In the centralized market, a typical miner i chooses the consumption of the CM good, x_t^i, the amount of new cryptocurrency to produce, δ_t^i, and fiat money holdings, $m_t^{m,i}$, and sells all the newly produced cryptocurrencies at price p_t after production. The maximization problem of a typical miner i is represented by:

$$W_t(m_{t-1}^{m,i}) = \max_{\delta_t^i, m_t^{m,i}} \quad p_t^c \delta_t^i - c(\delta_t^i, M_{t-1}^c) + p_t^m (m_{t-1}^{m,i} - m_t^{m,i}) + \beta W_{t+1}(m_t^{m,i}) \tag{E.4}$$

Solving the problem (E.4), we have:

$$p_t^c = \frac{\partial c(\delta_t^i, M_{t-1}^c)}{\partial \delta_t^i} \tag{E.5}$$

$$-p_t^m + \beta p_{t+1}^m \leq 0 \quad \text{“}=\text{”} \quad \text{if} \quad m_t^{m,i} > 0 \tag{E.6}$$

From (E.5), a miner will produce $\delta_t^i = \max\,[\,0, f(p_t^c, M_{t-1}^c)]$ units of cryptocurrency in period t. From (E.6), a miner will not hold any unit of fiat money when it is costly to carry, i.e., $p_t^m > \beta p_{t+1}^m$. Intuitively, miners remain idle in the second sub-period, thus, they do not have an incentive to carry fiat money out of the centralized market. As the stock of fiat money grows at $\gamma > \beta, m_t^{m,i} = 0$ in equilibrium, $\forall t$. Therefore, the equilibrium outcomes remain the same as those of the two-currency economy in the main context, in which miners are assumed not to carry fiat money.

Appendix F. An Example of the Cost Function

In this section, I describe the equilibrium outcomes of the cryptocurrency-only economy with a specific form of the production cost function, $c(\delta_t^i, M_{t-1})$, that is specified in Example 2.1.

Under Assumption 2.2 and Example 2.1, a typical miner i produces δ_t^i units of cryptocurrency in period t, given p_t and M_{t-1}, such that:

$$\delta_t^i = \max[0, \frac{p_t - DM_{t-1}}{2B}] \tag{F.1}$$

From (F.1), the number of newly produced cryptocurrency in each period depends on the value and the stock of cryptocurrency. A miner will not produce any cryptocurrency if $p_t - DM_{t-1} \leq 0$. Further, the aggregate new cryptocurrency in period t, Δ_t, becomes:

$$\Delta_t = \int_0^1 \delta_t^i di = \max[0, \frac{p_t - DM_{t-1}}{2B}] \tag{F.2}$$

Proposition F.1. *Under Assumption 2.1 and Example 2.1, there exists a unique stationary monetary equilibrium, in which the price of cryptocurrency is constant. The equilibrium outcomes are characterized by:*

$$\frac{1-\beta(1-\kappa)}{\sigma\beta(1-\kappa)} = [\frac{u' \circ \omega^{-1}(\beta z^{ss}(1-\kappa))}{\omega' \circ \omega^{-1}(\beta z^{ss}(1-\kappa))} - 1] \tag{F.3}$$

$$p^{ss} = (D + 2B\kappa)M^{ss} \tag{F.4}$$

$$1 + \frac{1-\beta(1-\kappa)}{\sigma\beta(1-\kappa)} = \frac{u'(q^{ss})}{\omega'(q^{ss})} \tag{F.5}$$

$$\Delta^{ss} = \kappa M^{ss} \tag{F.6}$$

[Proof of Proposition F.1]

Proof. Everything follows the Proof of Proposition 1 by replacing the aggregate production Δ_t with (F.2). Under Assumption 2.1 and Example 2.1, and given the functional forms and model parameters, the equilibrium outcomes can be uniquely determined by (F.3)-(F.6).

□

Appendix G. Comparative Statics

I obtain the comparative statics in Table 1 using the Cramer's Rule, following Zhu and Hendry (2019). In particular, consider the equilibrium conditions:

$$\begin{aligned} i_m &= \alpha_1\sigma L(\frac{z_m}{\gamma}) + \alpha_3\sigma L(\frac{z_m}{\gamma} + \frac{(1-\kappa)z_c}{1+\mu}) \\ i_c &= \alpha_2\sigma L(\frac{(1-\kappa)z_c}{1+\mu}) + \alpha_3\sigma L(\frac{z_m}{\gamma} + \frac{(1-\kappa)z_c}{1+\mu}) \end{aligned}$$

Taking derivatives of both equations with respect to i_m, we have

$$1 = \alpha_1\sigma L'(\frac{z_m}{\gamma})\frac{1}{\gamma}\frac{dz_m}{di_m} + \alpha_3\sigma L'(\frac{z_m}{\gamma} + \frac{(1-\kappa)z_c}{1+\mu})(\frac{1}{\gamma}\frac{dz_m}{di_m} + \frac{1-\kappa}{1+\mu}\frac{dz_c}{di_m}) \tag{G.1}$$

$$0 \;=\; \alpha_2\sigma L'(\frac{(1-\kappa)z_c}{1+\mu})\frac{1-\kappa}{1+\mu}\frac{dz_c}{di_m} + \alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1}{\gamma}\frac{dz_m}{di_m}+\frac{1-\kappa}{1+\mu}\frac{dz_c}{di_m}) \qquad \text{(G.2)}$$

Equations (G.1) and (G.2) can be written as:

$$\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}\alpha_1\sigma L'(\frac{z_m}{\gamma})\frac{1}{\gamma}+\alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1}{\gamma}) & \alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1-\kappa}{1+\mu})\\ \alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1}{\gamma}) & \alpha_2\sigma L'(\frac{(1-\kappa)z_c}{1+\mu})\frac{1-\kappa}{1+\mu}++\alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1-\kappa}{1+\mu})\end{bmatrix}\begin{bmatrix}\frac{dz_m}{di_m}\\ \frac{dz_c}{di_m}\end{bmatrix}$$

$$\text{Let}\;\; D = det\begin{pmatrix}\alpha_1\sigma L'(\frac{z_m}{\gamma})\frac{1}{\gamma}+\alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1}{\gamma}) & \alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1-\kappa}{1+\mu})\\ \alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1}{\gamma}) & \alpha_2\sigma L'(\frac{(1-\kappa)z_c}{1+\mu})\frac{1-\kappa}{1+\mu}+\alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1-\kappa}{1+\mu})\end{pmatrix}$$

$$\begin{aligned}&= \alpha_1\sigma L'(\frac{z_m}{\gamma})\frac{1}{\gamma}\alpha_2\sigma L'(\frac{(1-\kappa)z_c}{1+\mu})\frac{1-\kappa}{1+\mu} + \alpha_1\sigma L'(\frac{z_m}{\gamma})\frac{1}{\gamma}\alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1-\kappa}{1+\mu})\\ &\quad + \alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1}{\gamma})\alpha_2\sigma L'(\frac{(1-\kappa)z_c}{1+\mu})\frac{1-\kappa}{1+\mu}\end{aligned}$$

$$\text{Let}\;\; D_m = det\begin{pmatrix}1 & \alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1-\kappa}{1+\mu})\\ 0 & \alpha_2\sigma L'(\frac{(1-\kappa)z_c}{1+\mu})\frac{1-\kappa}{1+\mu}+\alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1-\kappa}{1+\mu})\end{pmatrix}$$

$$= \alpha_2\sigma L'(\frac{(1-\kappa)z_c}{1+\mu})\frac{1-\kappa}{1+\mu} + \alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1-\kappa}{1+\mu})$$

$$\text{Let}\;\; D_c = det\begin{pmatrix}\alpha_1\sigma L'(\frac{z_m}{\gamma})\frac{1}{\gamma}+\alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1}{\gamma}) & 1\\ \alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1}{\gamma}) & 0\end{pmatrix}$$

$$= -\alpha_3\sigma L'(\frac{z_m}{\gamma}+\frac{(1-\kappa)z_c}{1+\mu})(\frac{1}{\gamma})$$

Using the Cramer's Rule, $\frac{dz_m}{di_m} = \frac{D_m}{D} < 0, \frac{dz_c}{di_m} = \frac{D_c}{D} > 0$. Similarly, taking derivatives of the equilibrium conditions with respect to other parameters and repeating the above steps, we can obtain the rest of Table 1.