On the Coexistence of Cryptocurrency and Fiat Money

Zhixiu Yu*

June 15, 2021

Abstract

Cryptocurrency is private money and is costly to produce. In this paper, I ask whether cryptocurrency can serve as a medium of exchange, and whether it can coexist with fiat money as a widely accepted medium of exchange. To answer these questions, I develop two search-theoretic models: a model of monetary exchange in an economy with cryptocurrency only and a model of currency competition between cryptocurrency and fiat money. In my models, profit-maximizing miners produce cryptocurrency. In the economy with cryptocurrency only, unlike fiat money models, there is no equilibrium in which the stock of cryptocurrency grows at a constant rate. In a stationary equilibrium in which cryptocurrency is valued, the stock of cryptocurrency must be constant. In the two-currency economy, cryptocurrency and fiat money differ in terms of issuers, production costs, supply rules, and degrees of acceptability in decentralized markets. Different from the traditional two-fiat money models in which currencies have the same rate of return in equilibrium, cryptocurrency and fiat money can circulate in equilibrium with different rates of return. Further, 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, 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. Since Bitcoin was introduced in 2008, the market for cryptocurrencies has evolved dramatically. In July 2020, Bitcoin prices exceeded $10,000, and the total market capitalization of over 5,000 cryptocurrencies reached $320 billion.[1] Recently, a U.S. Federal Court has declared that Bitcoin is a form of "money"under the Washington, D.C. Money Transmitters Act.[2] Similar to fiat money, cryptocurrencies are intrinsically worthless. Unlike most common forms of fiat currency such as dollars or euros, cryptocurrencies are not backed by a central bank or any government authorities. The supply rules of cryptocurrencies are 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-issued currency problem.[3]

In recent years, as the number of companies that accept Bitcoin as a form of payment for goods and services has grown to include AT&T, Whole Foods, KFC Canada, Expedia, Subway, PayPal, and Microsoft, cryptocurrency has become an increasingly accepted form of monetary transaction.[4] The growing acceptance suggests cryptocurrency has the potential to disrupt the traditional monetary system, and this raises several questions: Can cryptocurrency serve as a medium of exchange? Can cryptocurrency coexist as a widely accepted medium of change with an asset that costs nothing to produce, such as fiat money? Under what conditions can cryptocurrency and fiat money both be used as media of exchange? 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 cryptocurrency only to study the role of cryptocurrency as a medium of exchange. My framework builds on 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 environment by adding a new type of agents—miners—who are able to produce cryptocurrency to maximize their profits. The Lagos-Wright framework is particularly insightful for addressing currency issues since it explicitly formalizes a medium of exchange essential in facilitating trades

[1] Source: `https://coinmarketcap.com/all/views/all/`.

[2] On July 24, 2020, Chief Judge Beryl A. Howell says "Money commonly means a medium of exchange, method of payment, or store of value. Bitcoin is these things." See more on *Bloomberg Law*.

[3] See Araujo and Camargo (2006, 2008) for discussion on the over-issued problem of fiat money.

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

in the decentralized trading arrangement.[5] In addition, the Lagos-Wright framework is amendable to analysis and allows me to incorporate a miner sector while keeping the distribution of currency holdings analytically tractable.

My model highlights two key attributes of cryptocurrency: it is private money, and it is costly to produce. I refer to issuers of cryptocurrency as miners. I assume that miners can use the technology to produce cryptocurrency, and the cost of producing cryptocurrency increases in both the amount of newly produced units and the existing stock of cryptocurrency in the market. 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.[6] Thus, the cost of mining the same amount of Bitcoin gets more expensive as more Bitcoin is minted. 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.[7]

Moreover, I model the cryptocurrency law of motion by assuming that the stock of cryptocurrency in each period is determined by the newly produced cryptocurrencies and by the depreciation from the last period. The amount of new cryptocurrency is determined by miners' production, 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 lose because people sent it to a wrong address, or lost or discarded device, or forgot their password which has complicated strings, etc.[8] According to Chainalysis, a blockchain analysis company, about 23% of all Bitcoins currently in circulation may be lost forever. Unlike fiat money, such as cash, which can be reused after getting lost, once a cryptocurrency is lost, it might be lost forever and can not be

[5]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).

[6]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 number of 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`.

[7]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 the cryptocurrency role as a speculative asset (e.g., Zhou (2020)), in the context of search-theoretic models. Unlike these papers, I emphasize the costly-to-produce feature of cryptocurrency to study its role as the medium of exchange and coexistence conditions of fiat money and cryptocurrency.

[8]For more information on the issue of cryptocurrency loss, see `https://medium.com/luno-money/where-do-lost-bitcoins-go-7e8dd24abd0f`.

reused by other people.[9]

In the economy with cryptocurrency only, I show that there exists a monetary stationary equilibrium. This is similar to what happens in fiat money models (e.g., Lagos and Wright (2003, 2005)). However, unlike fiat currency models, there is no monetary stationary equilibrium in which the stock of cryptocurrency grows at a constant rate. A key result of my economy with cryptocurrency only is that, when the aggregate new cryptocurrency is endogenously determined and the production cost increases in both the newly produced units and the existing stock, in equilibrium, the stock of cryptocurrency must be constant. That is, all the newly produced cryptocurrencies only replace the depreciation in each period. My results show that the costly produced cryptocurrency is very different from fiat money, since in the economy with fiat money only, there is an equilibrium in which the growth rate of fiat money supply is positive (e.g., Lagos and Wright (2005), Rocheteau and Wright (2005)), but in the economy with cryptocurrency only, there is no such equilibrium.

Next, to explore the coexistence of cryptocurrency and fiat money, I develop a search model of currency competition by extending my cryptocurrency-only model through adding fiat money and multiple decentralized markets into the economy. In this model, fiat money and cryptocurrency differ from each other in their 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). In particular, fiat money is issued by the government according to a deterministic growth rule with no associated costs, and changes in fiat money supply are injected or withdrawn in a lump-sum fashion to agents. In comparison, cryptocurrency is costly to produce, and its net circulation in each period is determined by both the miners' production and the currency depreciation. In addition, 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 the DM1 (e.g., transactions that accept cash only or involve the government authorities); agents can only trade with cryptocurrency in the DM2 (e.g., online Bitcoin stores or black markets where fiat money is not used); and agents can trade with both currencies in the DM3 (e.g., KFC Canada, PayPal, etc.). Agents randomly enter one of the decentralized markets with a certain probability in each period. 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).[10] The assumption of currencies with different degrees of acceptability in markets is akin to the cash-in-advance assumptions in

[9]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 lost because the thieves have access to it. For literature on identity theft and currency security, see e.g., **?**, Kahn and Roberds (2008) and Kahn et al. (2020).

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

Lucas (1982), which constrain agents to use one type of currency in a particular trade. It is also similar to the models of private and fiat monies, e.g., Choi and Rocheteau (2020b) and Zhu and Hendry (2019), in which two currencies differ in their degrees of acceptability in decentralized meetings.

In the economy of cryptocurrency and fiat money, I show that, depending on the fundamentals and parameters of the model, there are currency regimes with neither, both, or only one of the currencies that are valued and circulating. This is similar to what happens in multiple-fiat currency models (e.g., Camera et al. (2004) and Engineer (2000)). In my two-currency economy, the probability that agents visit each decentralized market is exogenous, but 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. Moreover, 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. 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.

I then analyze the coexistence of cryptocurrency and fiat money as media of exchange under the following cases. In the first case, there are completely segmented decentralized markets in the economy, in which agents can only trade with fiat money in the DM1 and only trade with cryptocurrency in the DM2. In this set-up, two currencies coexist with different rates of return, and there is a dichotomy between two currencies' sectors. That is, the real value of cryptocurrency is determined independently from the real value of fiat money, and the monetary policy on the fiat money growth rule has no effect on cryptocurrency use. 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, suppose there are only DM2 and DM3 in the economy. In that case, cryptocurrency has an inherent advantage relative to fiat money since agents can trade with cryptocurrency everywhere but trade with fiat money only in the DM3. 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. For example, suppose fiat money has an inherent advantage relative to cryptocurrency. In that case, cryptocurrency has a higher rate of return than fiat money in a stationary equilibrium in which both currencies are valued. Intuitively, agents will carry the currency that can be used everywhere in order to facilitate trades in decentralized markets, so the rate of return on less acceptable currency must be sufficiently high

in order to give agents enough incentive to carry it as well.

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 in decentralized markets and whether the government can commit to maintaining the targeted fiat money growth rule. Cryptocurrency is costly to produce. Banning cryptocurrency can avoid the resource waste on production but may worsen the total welfare since agents can only trade using fiat money in all decentralized meetings and, thus, there is no trade surplus in the DM2, where only cryptocurrency is accepted as the payment method. 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 in decentralized markets is small and the government can maintain sufficient low inflation, then banning cryptocurrency would be welfare-enhancing. There would be welfare gains from avoiding resource waste on producing cryptocurrency and from consuming more goods in the markets where fiat money is used, which outweigh the welfare loss from no trade surplus in the DM2. Efficient allocations in decentralized markets can be achieved when monetary policy follows the Friedman rule if cryptocurrency is banned. Otherwise, if the government tends to overissue fiat money, then banning cryptocurrency would worsen the total welfare since there would be large welfare loss from consuming less using fiat money in decentralized markets and no trade surplus in the DM2.

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) study the competition between fiat money and capital as means of payment and show that two assets 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, even if one is dominated by the other in the rate of return. This is driven by the assumption that two currencies have different degrees of acceptability in decentralized markets. Thus, each currency is essential in some transactions.[11]

The literature has also emphasized the inherent properties of the use of money. Velde et al. (1999) develop a model where two types of commodity money, light and heavy coins, are used as media of exchange. By introducing private information, they show that Gresham's Law—"Bad money drives out good money"— holds in the way that bad money is always traded while good money is traded if and only if the seller is informed. Camera et al. (2004) study the currency

[11]Hu and Rocheteau (2013) provide a summary of several approaches that explain different rate-of-return across assets.

competition between two types of fiat money: safe money and risky money that is characterized by a purchasing power risk. In contrast, their model produces the highest velocity for the good money—agents favor spending the safe money and holding on to the risky one for subsequent trades, where Gresham's Law has been reversed. Unlike those papers, my results show that both bad and good assets can circulate. Cryptocurrency, which is, in some sense, inferior in production costs and acceptability in decentralized meetings, can coexist with fiat money, when appropriate monetary policy is implemented. Thus, Gresham's Law does not hold in my paper. 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. Here, I explore other properties of currencies, such as growth rates 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.

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 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 for issuing tokens. My emphasis is different from theirs. I focus on the coexistence of cryptocurrency and fiat money in stationary equilibrium, and two currencies can coexist with different rates of return in my model. 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 (electronic money) is costless to produce in Zhu and Hendry (2019). Thus, these papers cannot have an analog of the monetary equilibrium in which the stock of cryptocurrency must be constant. Moreover, my model structure is close to that of Fernández-Villaverde and Sanches (2019) in that new private money is supplied by profit-maximizing agents who have a technology to produce in each period. In their paper, miners produce their own brands of private monies, and the costs of producing each brand of private money increase only in the newly produced units. Unlike their paper, miners in my model produce the same type of cryptocurrency, and the production cost increases in both the amount of newly produced units and the existing stock. Together with currency depreciation, these novelties make my model different from fiat money models since there is no stationary equilibrium in which

the growth rate of cryptocurrency supply is positive.

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 (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 is 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 deposit serves a socially useful insurance role and is privately useful since it 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.

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

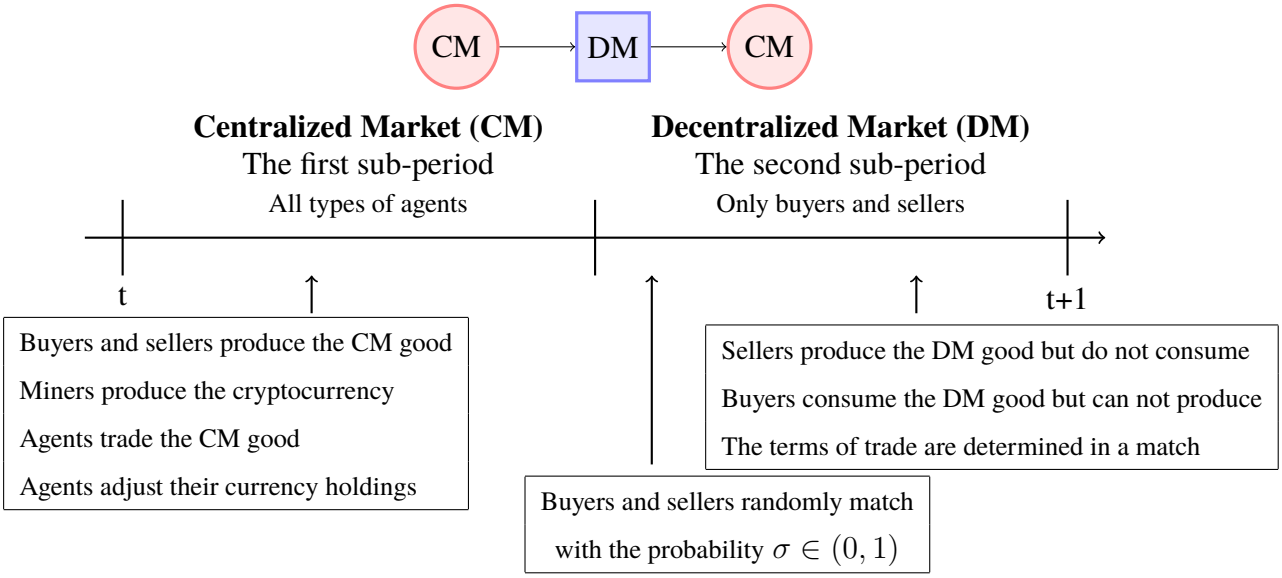
There are three types of infinitely lived agents in the economy: *buyers, sellers*, and *miners*. Each of them are populated with a [0,1]-continuum, and agents' types are permanent. Time is discrete and continues forever. Agents discount the future between periods with a discount factor $\beta \in (0, 1)$, and β is common across all agents. Each period is divided into two sub-periods, in which different economic activities take place.[12] 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 the CM good 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 technology and sell all the newly produced units to sellers and buyers right after production. All agents adjust their cryptocurrency holdings by producing or consuming the CM good in the centralized market. The

[12]My model framework is built on Lagos and Wright (2005), and the particular market structure is similar to the one in Fernández-Villaverde and Sanches (2019).

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.

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



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.[13] 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 (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.

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.

[13] 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.

The preferences of a typical buyer, seller, and miner are represented by the following quasi-linear instantaneous utility functions:

$$\begin{aligned} U^b(x_t^b, q_t) &= x_t^b + u(q_t) \\ U^s(x_t^s, q_t) &= x_t^s - \omega(q_t) \\ U^i(x_t^i) &= x_t^i \end{aligned}$$

where b, s, i refer to a typical buyer, seller, and miner, respectively. $u(q_t) : \mathbb{R}_+ \to \mathbb{R}$ 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. *$u(\cdot), \omega(\cdot)$ are twice continuously differentiable, s.t. $u'(q_t) > 0, u''(q_t) < 0, \omega'(q_t) > 0, \omega''(q_t) > 0$, and satisfy $u(0) = 0, u'(0) = \infty, \omega(0) = 0, \omega'(0) = 0$.*

2.1. Cryptocurrency

A medium of exchange is supplied only in the form of cryptocurrency. Cryptocurrency is costly to produce and perfectly divisible. Miners have the ability to produce it, and the production cost increases in both the newly produced units and the cryptocurrency stock in the market.

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

$$M_t = M_{t-1} + \underbrace{\Delta_t}_{\text{Newly produced}} - \underbrace{\pi M_{t-1}}_{\text{Depreciation}}, \quad \Delta_t \geq 0, \quad M_{-1} \text{ given.} \tag{1}$$

The aggregate new cryptocurrency, Δ_t, is endogenously determined by production decisions of miners, and the depreciation is intended to capture the idea that cryptocurrency is easier to lose, and the lost cryptocurrency can not be reused by others, e.g., Bitcoin.[14] Here I assume that a proportion $\pi \in (0, 1)$ of the cryptocurrency stock from the last period will be lost in each period.[15]

[14]The stolen cryptocurrency does not count as loss/depreciation because the thieves have access to it. In Appendix B, I alternatively model the cryptocurrency security as theft instead of loss, by assuming that cryptocurrency holdings are thieved by some agents. In that case, there is a unique stationary equilibrium in which no cryptocurrency is produced.

[15]Unlike my modeling of the currency depreciation, 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 intrinsically worthless and is not associated with any promise to exchange for goods in the future. Agents in the economy 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.

2.2. *Buyers and sellers*

First, I describe the problems of buyers and sellers in the 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, π, of the cryptocurrency holdings that an agent brings to the centralized market loses. 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:

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

$$W_t^s(m_{t-1}^s) = \max_{x_t^s, m_t^s} \quad x_t^s + V_t^s(m_t^s), \qquad s.t. \qquad x_t^s + p_t m_t^s = p_t(1-\pi)m_{t-1}^s \tag{3}$$

The above CM value functions can be rearranged as:

$$W_t^j(m_{t-1}^j) = p_t(1-\pi)m_{t-1}^j + \underbrace{\max_{m_t^j \in \mathbb{R}_+} -p_t m_t^j + V_t^j(m_t^j)}_{W_t^j(0)}, \quad j \in \{b, s\} \tag{4}$$

From (4), an agent's choice of cryptocurrency holdings at t, m_t^j, is independent of the initial cryptocurrency holdings when entering the centralized market, m_{t-1}^j, and the cryptocurrency loss $\pi m_{t-1}^j,\ j \in \{b, s\}$. 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.[16]

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 of (4) with respect to $m_t^j,\ j \in \{b, s\}$.

$$-p_t + V_t^{b'}(m_t^b) \leq 0 \qquad \text{“}=\text{”} \quad \text{if} \quad m_t^b > 0 \tag{5}$$

$$-p_t + V_t^{s'}(m_t^s) \leq 0 \qquad \text{“}=\text{”} \quad \text{if} \quad m_t^s > 0 \tag{6}$$

where $V_t^{b'}(m_t^b)$ and $V_t^{s'}(m_t^s)$ are determined by the decentralized market problems of agents.

*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:

$$V_t^b(m_t^b) = \max_{q_t, d_t} \quad \sigma[u(q_t) + \beta W_{t+1}^b(m_t^b - d_t)] + (1-\sigma)\beta W_{t+1}^b(m_t^b) \tag{7}$$

$$V_t^s(m_t^s) = \sigma[-\omega(q_t) + \beta W_{t+1}^s(m_t^s + d_t)] + (1-\sigma)\beta W_{t+1}^s(m_t^s) \tag{8}$$

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, (q_t, d_t). 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

[16]The CM value function (4) remains the same if I alternatively assume that with the probability π, agents lose all the cryptocurrency holdings from the last period. Specifically, with the probability π, 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 $1-\pi$, 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: $p_t m_{t-1}^j + W_t^j(0)$. Then the CM value function is: $\pi W_t^j(0) + (1-\pi)[p_t m_{t-1}^j + W_t^j(0)] = (1-\pi)p_t m_{t-1}^j + W_t^j(0),\ j \in \{b, s\}$.

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 the following problem.

$$\begin{aligned} \max_{q_t, d_t} \quad & u(q_t) + \beta W_{t+1}^b(m_t^b - d_t) \\ s.t. \quad & -\omega(q_t) + \beta W_{t+1}^s(m_t^s + d_t) \geq \beta W_{t+1}^s(m_t^s) \\ & d_t \leq m_t^b \end{aligned} \tag{9}$$

where the first inequality is the seller's participation constraint and the second one is the buyer's liquidity constraint. Substituting (4), problem (9) can be simplified as follows.

$$\begin{aligned} \max_{q_t, d_t} \quad & u(q_t) - \beta p_{t+1}(1-\pi) d_t \\ s.t. \quad & -\omega(q_t) + \beta p_{t+1}(1-\pi) d_t \geq 0 \\ & d_t \leq m_t^b \end{aligned} \tag{10}$$

According to (10), the buyer's choices of (q_t, d_t) do not depend on the seller's cryptocurrency holdings, m_t^s. The optimal offer is such that seller's participation constraint holds with equality. Under Assumption 2.1, there exists a level of the traded amount of the DM good, $q^* = \text{argmax}\,[u(q_t) - \omega(q_t)]$ and $q^* > 0$, 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 make enough payment to get q^*, i.e., $q_t = q^*, d_t = m_t^* = \frac{\omega(q^*)}{\beta p_{t+1}(1-\pi)}$. 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., $d_t = m_t^b, q_t = \hat{q}_t = \omega^{-1}(\beta p_{t+1}(1-\pi) m_t^b)$ and $\hat{q}_t < q^*$. The solutions to problem (10) are summarized in the following Lemma.

Lemma 2.2. *The terms of trade, (q_t, d_t), that solve problem (10) are given by:*

$$q_t(m_t^b) = \begin{cases} q^* & if \quad m_t^b \geq m_t^* \\ \hat{q}_t & if \quad m_t^b < m_t^* \end{cases} \qquad d_t(m_t^b) = \begin{cases} m_t^* & if \quad m_t^b \geq m_t^* \\ m_t^b & if \quad m_t^b < m_t^* \end{cases} \tag{11}$$

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

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

Next, given (4) and Lemma 2.2, the DM value functions (7)-(8) can be rewritten as follows:

$$V_t^b(m_t^b) = \beta(p_{t+1}(1-\pi)m_t^b + W_{t+1}^b(0)) + \underbrace{\sigma[u(q_t(m_t^b)) - \omega(q_t(m_t^b))]}_{\text{a buyer's expected surplus in the DM, } v_t(m_t^b)} \tag{12}$$

$$V_t^s(m_t^s) = \beta(p_{t+1}(1-\pi)m_t^s + W_{t+1}^s(0)) + \underbrace{0}_{\text{a seller's expected surplus in the DM}} \tag{13}$$

$$\text{where } v_t(m_t^b) = \begin{cases} \sigma[u(q^*) - \omega(q^*)] & if \quad m_t^b \geq m_t^* \\ \sigma[u(\hat{q}(m_t^b)) - \omega(\hat{q}_t(m_t^b))],\ \hat{q}_t = \omega^{-1}(\beta p_{t+1}(1-\pi)m_t^b) & if \quad m_t^b < m_t^* \end{cases}$$

The first terms on the right-hand side (RHS) of (12)-(13) result from the linearity of the CM value functions, while the second terms represent the expected surplus of an agent in the decentralized market. 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.[17]

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

Substituting (12)-(13) into (4), the optimal cryptocurrency holdings of a buyer and seller are then given by the solutions to:

$$W_t^b(m_{t-1}^b) = \max_{m_t^b \in \mathbb{R}_+} - \underbrace{(p_t - p_{t+1}\beta(1-\pi))m_t^b}_{\text{the cost of carrying money to next period}} + \underbrace{\sigma[u(q_t(m_t^b)) - \omega(q_t(m_t^b))]}_{\text{the expected surplus in the DM} = v_t(m_t^b)} \tag{14}$$

$$W_t^s(m_{t-1}^s) = \max_{m_t^s \in \mathbb{R}_+} - \underbrace{(p_t - p_{t+1}\beta(1-\pi))m_t^s}_{\text{the cost of carrying money to next period}} + \underbrace{0}_{\text{the expected surplus in the DM}} \tag{15}$$

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. Since sellers have no surplus in the decentralized market, there is no strict incentive for them to carry cryptocurrency out of the centralized market. From (14)-(15), cryptocurrency is costly to carry when $\frac{p_t}{p_{t+1}} > \beta(1-\pi)$.

The optimal cryptocurrency holdings for a buyer and seller can be obtained by taking the first-order conditions of (14)-(15) with respect to m_t^b and m_t^s, respectively.

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

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

$$-p_t + \beta p_{t+1}(1-\pi) + v_t^{'}(m_t^b) \leq 0 \qquad \text{“ = ” } \textit{if} \quad m_t^b > 0 \tag{16}$$

$$-p_t + \beta p_{t+1}(1-\pi) \leq 0 \qquad \text{“ = ” } \textit{if} \quad m_t^s > 0 \tag{17}$$

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

The term $v_t^{'}(m_t^b)$ is a liquidity factor that captures the expected discounted payoff of holding cryptocurrency to facilitate transactions in the decentralized market.[18] 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 (16)-(17), there will be no solution when $\frac{p_t}{p_{t+1}} < \beta(1-\pi)$. When cryptocurrency is costless to carry, i.e., $\frac{p_t}{p_{t+1}} = \beta(1-\pi)$, buyers will carry enough cryptocurrency to get q^* in the decentralized match. In that case, $v_t^{'}(m_t^b) = 0$, and there is no value for buyers to carry an additional unit of cryptocurrency to the decentralized market. In contrast, when cryptocurrency is costly to carry, i.e., $\frac{p_t}{p_{t+1}} > \beta(1-\pi)$, sellers will not hold any unit of cryptocurrency, and buyers will only carry what they expect to spend in the decentralized meeting. Buyers will spend all the cryptocurrency holdings to purchase the DM good, $\hat{q}_t < q^*$, in a match. In that case, $v_t^{'}(m_t^b) > 0$, and buyers value an additional unit of cryptocurrency that they carry to the decentralized market.

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

$$\frac{p_t}{p_{t+1}} - \beta(1-\pi) = \beta\sigma(1-\pi)[\frac{u^{'} \circ \omega^{-1}(\beta p_{t+1}(1-\pi)m_t^b)}{\omega^{'} \circ \omega^{-1}(\beta p_{t+1}(1-\pi)m_t^b)} - 1] \tag{18}$$

*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

[18] Equivalently, we can derive the optimal cryptocurrency holdings for a buyer and seller using the first-order conditions (5)-(6) and the DM value functions (12)-(13). The resulting conditions will be same as (16)-(17), with $V_t^{b'}(m_t^b) = \beta p_{t+1}(1-\pi) + v_t^{'}(m_t^b)$ and $V_t^{s'}(m_t^s) = \beta p_{t+1}(1-\pi)$.

on the newly produced units δ_t^i, and the existing cryptocurrency stock, M_{t-1}.[19] Miners sell all newly produced cryptocurrencies at price p_t right after production. Then the maximization problem of a typical miner is represented by:

$$\begin{aligned} \max_{x_t^i, \delta_t^i} \quad & \sum_{t=0}^{\infty} \beta^t x_t^i \\ \text{s.t.} \quad & x_t^i \leq p_t \delta_t^i - c(\delta_t^i, M_{t-1}) \quad \forall t \\ & x_t^i, \delta_t^i \geq 0 \qquad \forall t \end{aligned} \tag{19}$$

where $c : \mathbb{R}^2 \to \mathbb{R}$ is increasing, convex, and twice differentiable.

Assumption 2.2. $c(\delta_t, M_{t-1}) = DM_{t-1}\delta_t + B\delta_t^2, \quad B, D > 0.$

Given (19), the miner's problem at each period t can be written as follows.

$$\max_{\delta_t^i \geq 0} \quad p_t \delta_t^i - c(\delta_t^i, M_{t-1}) \tag{20}$$

The amount of new cryptocurrency, δ_t^i, that a miner produces in period t can be obtained by taking the first-order condition of (20).

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:*

$$\delta_t^i = \max[0, \frac{p_t - DM_{t-1}}{2B}] \tag{21}$$

From (21), 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:

$$\Delta_t = \int_0^1 \delta_t^i di = \max[0, \frac{p_t - DM_{t-1}}{2B}] \tag{22}$$

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

[19] Unlike my modeling of the cryptocurrency production costs, Choi and Rocheteau (2020a) develop a model in which private monies are produced according to a time-consuming technology. In addition, there are opportunity costs for miners due to occupation choice.

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 a sequence of value of cryptocurrency* $\{p_t\}_{t=0}^{\infty}$*, such that for all* $t \geq 0$*,*

1. $x_t^b, m_t^b, x_t^s, m_t^s$ *solve problems (2)-(3) and (7)-(8) for buyers and sellers;*
2. q_t, d_t *solve problem (9) and satisfy (11);*
3. x_t^i, δ_t^i *solve problem (19) for miners;*
4. *cryptocurrency law of motion is satisfied:*
   $M_t = (1-\pi)M_{t-1} + \Delta_t$, *where* Δ_t *satisfies (22);*
5. *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. *centralized good market clear:*
   $\int_0^1 x_t^b db + \int_0^1 x_t^s ds + \int_0^1 x_t^i di + \int_0^1 c(\delta_t^i, M_{t-1}) di = 0$.

Definition 2. *A monetary equilibrium is an equilibrium in which cryptocurrency is valued.*

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.

Suppose the stock of cryptocurrency grows at a constant rate $\mu \in \mathbb{R}$, i.e., $M_{t+1} = (1+\mu)M_t$. From cryptocurrency law of motion (1), $\Delta_t = (\mu + \pi)M_{t-1}$. Since Δ_t cannot be negative, there is no solution to equilibrium when $\mu < -\pi$, and no cryptocurrency is produced when $\mu = -\pi$.

3.1.1. Constant Cryptocurrency Stock

First, I examine the stationary equilibrium in which the stock of cryptocurrency is constant, i.e., $\mu = 0$ and $M_{t+1} = M_t = M^{ss}\ \forall t$. Then $\Delta = \pi M^{ss}$.

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

$$\frac{1-\beta(1-\pi)}{\sigma\beta(1-\pi)} = [\frac{u' \circ \omega^{-1}(\beta z^{ss}(1-\pi))}{\omega' \circ \omega^{-1}(\beta z^{ss}(1-\pi))} - 1] \tag{23}$$

$$p^{ss} = (D + 2B\pi)M^{ss} \tag{24}$$

$$1 + \frac{1-\beta(1-\pi)}{\sigma\beta(1-\pi)} = \frac{u'(q^{ss})}{\omega'(q^{ss})} \tag{25}$$

$$\Delta^{ss} = \pi M^{ss} \tag{26}$$

Under Assumption 2.1, $\frac{u'(q)}{\omega'(q)}$ goes to infinity as q approaches zero and equals 1 when $q = q^*$. $\frac{u'(q_t)}{\omega'(q_t)}$ is decreasing in q_t for $q_t < q^*$. Therefore, there is a unique set of equilibrium outcomes that satisfy (23)-(26) in Proposition 1.

Similar to what happens in fiat money models (e.g., Lagos and Wright (2005)), there exists a stationary equilibrium in which cryptocurrency is valued. In this equilibrium, the stock of cryptocurrency remains constant, and all the newly produced cryptocurrencies only replace the currency depreciation.

3.1.2. ***Time-Varying Cryptocurrency Stock***

Next, I examine the stationary equilibrium in which the stock of cryptocurrency grows at a constant rate, i.e., $\mu \neq 0$ and $\mu > -\pi$.[20] Following the cryptocurrency law of motion and Lemma 2.6, Δ_t satisfies the aggregate production (22) and $\Delta_t = (\mu + \pi)M_{t-1}$ in equilibrium.

Proposition 2. *Under Assumptions 2.1 and 2.2, there does not exist a monetary stationary equilibrium in which the stock of cryptocurrency grows at a constant rate.*

Proposition 2 presents a key result of the economy where cryptocurrency is costly to produce and the aggregate supply is endogenously determined. That is, the stock of cryptocurrency must remain constant in the stationary equilibrium in which cryptocurrency is valued and produced.

From Propositions 1 and 2, cryptocurrency – private money that is costly to produce – is very different from fiat money. Since in the fiat money models, there is an equilibrium in which the

[20] I assume $\mu > -\pi$ since I focus on the equilibrium where cryptocurrency is produced. In Appendix A.2, I show that there is a unique stationary equilibrium in which the stock of cryptocurrency shrinks at the depreciation rate, i.e., $\mu = -\pi$ and $M_{t+1} = (1-\pi)M_t$. In that equilibrium, there is no production of cryptocurrency, $\Delta = 0$.

growth rate of fiat money supply is positive (e.g., Lagos and Wright (2005), Rocheteau and Wright (2005)), but in the model with cryptocurrency, there is no such equilibrium.

4. Two-Currency Model

To explore the coexistence of two intrinsically worthless objects – cryptocurrency and fiat money – as media of exchange, I develop a currency competition model between two currencies. I extend my cryptocurrency-only model in Section 2 through 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 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 my two-currency economy, there are several features of cryptocurrency that distinguish it from fiat money. 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 the production cost increases in both the newly produced units and the existing cryptocurrency stock, while there is no cost for the government associated with issuing fiat money.
iii. The net circulation of cryptocurrency in each period is determined by both miners' production and the cryptocurrency depreciation, while fiat money is supplied by the government according to a deterministic growth rule.

[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. Agents who fail to pay taxes in the centralized market will be excluded from trades in the decentralized market.

iv. Cryptocurrency and fiat money have different degrees of acceptability in decentralized markets, which are specified in the following section.

*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.

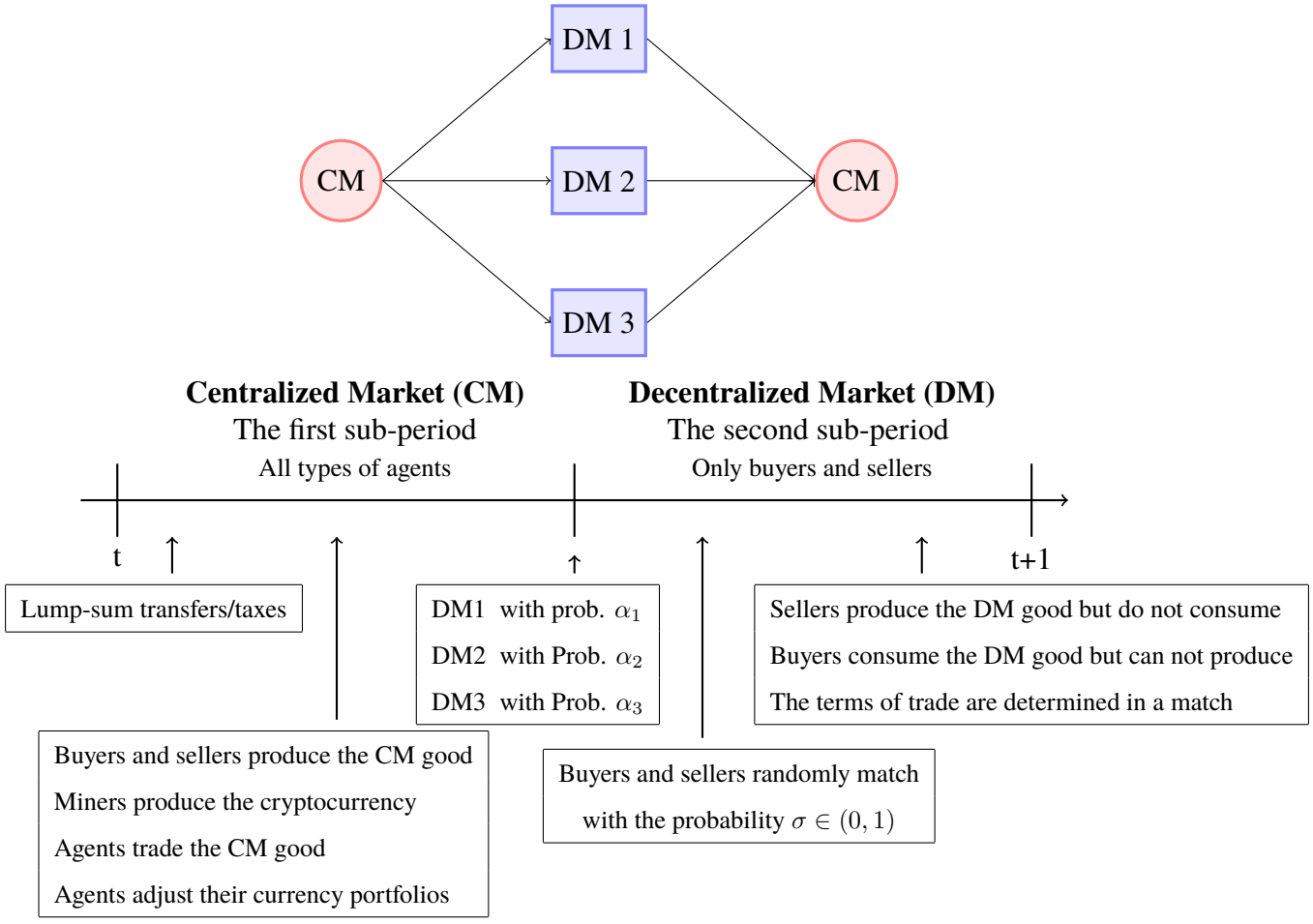
In the second sub-period, miners remain idle. Sellers and buyers randomly enter one of the three decentralized markets: DM1, DM2, and DM3, with probabilities α_1, α_2, and α_3, respectively, where $\alpha_{DM} \in [0,1]$ and $\sum_{DM=1}^{3} \alpha_{DM} = 1$, $\forall DM \in \{1,2,3\}$. The DM good is 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. Sellers can produce the DM good but do not want to consume; buyers want to consume the DM good but cannot produce. The utility and cost functions of the DM good, $u(\cdot), \omega(\cdot)$, satisfy Assumption 2.1, and the terms of trade are determined by a take-it-or-leave-it offer by the buyer in each match. 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 the DM1, agents can only trade with fiat money (e.g., transactions that accept cash only or involve the government authorities); in the DM2, agents can only trade with cryptocurrency (e.g., online Bitcoin stores and online black markets where fiat money is not used); and in the DM3, agents can trade with both currencies (e.g., KFC Canada, PayPal, etc.). Figure 2 summarizes the timing of events in a typical period of the two-currency economy.

[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).

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



4.3. Miners

I first describe the problem of miners in the two-currency economy. Miners are only active in the centralized market during the first sub-period.

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

$$\begin{aligned} \max_{x_t^i, \delta_t^i, m_t^{m,i}} \quad & \sum_{t=0}^{\infty} \beta^t x_t^i \\ \text{s.t.} \quad & x_t^i + p_t^m m_t^{m,i} \leq p_t^c \delta_t^i - c(\delta_t^i, M_{t-1}^c) + p_t^m m_{t-1}^{m,i} \quad \forall t \\ & x_t^i, \delta_t^i, m_t^{m,i} \geq 0 \qquad \forall t \end{aligned} \tag{27}$$

The production cost of cryptocurrency, $c(\cdot)$, has the same form as described in Assumption 2.2.

Since miners remain idle in the second sub-period, the value function of a miner can be written as follows.

$$W_t(m_{t-1}^{m,i}) = \max_{\delta_t^i, m_t^{m,i}} \quad p_t^c \delta_t^i - c(\delta_t^i, M_{t-1}^c) + p_t^m (m_{t-1}^{m,i} - m_t^{m,i}) + \beta W_{t+1}(m_t^{m,i}) \tag{28}$$

Under Assumption 2.2, we can solve problem (28) by taking the first-order conditions with respect to δ_t^i and $m_t^{m,i}$:

$$\delta_t^i = \max\,[\,0, \frac{p_t^c - DM_{t-1}^c}{2B}] \tag{29}$$

$$-p_t^m + \beta p_{t+1}^m \leq 0 \quad \text{“}=\text{”} \quad \text{if} \quad m_t^{m,i} > 0 \tag{30}$$

Same as Lemma 2.6 in the cryptocurrency-only economy, a miner's choice of the cryptocurrency production in each period depends only on the value and stock of cryptocurrency. Then the aggregate new cryptocurrency in period t, Δ_t, is the same as (22) with $p_t = p_t^c$ and $M_t = M_t^c$.

In addition, since miners remain idle in the second sub-period, they do not have an incentive to carry fiat money out of the centralized market. From (30), a miner will not hold any unit of fiat money when it is costly to carry, i.e., $p_t^m > \beta p_{t+1}^m$.

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, $j \in \{b, s\}$. In the first sub-period, agents interact in a centralized market. Due to different trading histories in decentralized markets, agents begin a period with different currency portfolios. A certain fraction, $\pi \in (0, 1)$, of the cryptocurrency holdings that an agent brings to the centralized market loses. Buyers receive lump-sum transfers/taxes from the government. In the centralized market, 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, $\mathbf{m}_{t-1}^j = (m_{t-1}^{m,j}, m_{t-1}^{c,j}) \in \mathbb{R}_+^2$, from the last period, and $V_t^j(\mathbf{m}_t^j)$ denote the value function

of an agent beginning the second sub-period with 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 buyer and seller in the centralized market are represented by:

$$W_t^b(\mathbf{m_{t-1}^b}) = \max_{x_t^b, \mathbf{m_t^b}} \; x_t^b + V_t^b(\mathbf{m_t^b}) \quad s.t. \quad x_t^b + \mathbf{p_t m_t^b} = p_t^m m_{t-1}^{m,b} + (1-\pi) p_t^c m_{t-1}^{c,b} + T_t \tag{31}$$

$$W_t^s(\mathbf{m_{t-1}^s}) = \max_{x_t^s, \mathbf{m_t^s}} \; x_t^s + V_t^s(\mathbf{m_t^s}) \quad s.t. \quad x_t^s + \mathbf{p_t m_t^s} = p_t^m m_{t-1}^{m,s} + (1-\pi) p_t^c m_{t-1}^{c,s} \tag{32}$$

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 (31)-(32) can be rearranged as follows.

$$W_t^b(\mathbf{m_{t-1}^b}) = p_t^m m_{t-1}^{m,b} + (1-\pi) p_t^c m_{t-1}^{c,b} + \underbrace{T_t + \max_{\mathbf{m_t^b} \in \mathbb{R}_+^2} -\mathbf{p_t m_t^b} + V_t^b(\mathbf{m_t^b})}_{W_t^b(0,0)} \tag{33}$$

$$W_t^s(\mathbf{m_{t-1}^s}) = p_t^m m_{t-1}^{m,s} + (1-\pi) p_t^c m_{t-1}^{c,s} + \underbrace{\max_{\mathbf{m_t^s} \in \mathbb{R}_+^2} -\mathbf{p_t m_t^s} + V_t^s(\mathbf{m_t^s})}_{W_t^s(0,0)} \tag{34}$$

Similar to the cryptocurrency-only economy, there is no wealth effect on an agent's choice of currency portfolio. The choice of $\mathbf{m}_t^j$ 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. Since search friction and trading process are the same across three decentralized markets, the DM problems for a typical buyer and seller are represented by:

$$\begin{aligned} V_t^b(\mathbf{m_t^b}) = \max_{(q_t^1, d_t^{1,m}), (q_t^2, d_t^{2,c}), (q_t^3, d_t^{3,m}, d_t^{3,c})} & \\ \alpha_1 \{\sigma[u(q_t^1) + \beta W_{t+1}^b(m_t^{m,b} - d_t^{1,m}, m_t^{c,b})] + (1-\sigma)\beta W_{t+1}^b(\mathbf{m}_t^b)\} & \\ + \alpha_2 \{\sigma[u(q_t^2) + \beta W_{t+1}^b(m_t^{m,b}, m_t^{c,b} - d_t^{2,c})] + (1-\sigma)\beta W_{t+1}^b(\mathbf{m}_t^b)\} & \\ + \alpha_3 \{\sigma[u(q_t^3) + \beta W_{t+1}^b(m_t^{m,b} - d_t^{3,m}, m_t^{c,b} - d_t^{3,c})] + (1-\sigma)\beta W_{t+1}^b(\mathbf{m_t^b})\} & \end{aligned} \tag{35}$$

$$
\begin{aligned}
V_t^s(\mathbf{m_t^s}) = \alpha_1\{\sigma[-\omega(q_t^1) + \beta W_{t+1}^s(m_t^{m,s} + d_t^{1,m}, m_t^{c,s})] + (1-\sigma)\beta W_{t+1}^s(\mathbf{m}_t^s)\} \\
+ \alpha_2\{\sigma[-\omega(q_t^2) + \beta W_{t+1}^s(m_t^{m,s}, m_t^{c,s} + d_t^{2,c})] + (1-\sigma)\beta W_{t+1}^s(\mathbf{m}_t^s)\} \\
+ \alpha_3\{\sigma[-\omega(q_t^3) + \beta W_{t+1}^s(m_t^{m,s} + d_t^{3,m}, m_t^{c,s} + d_t^{3,c})] + (1-\sigma)\beta W_{t+1}^s(\mathbf{m_t^s})\}
\end{aligned} \tag{36}
$$

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, $d_t^{1,m}$ denotes the transfer of fiat money in the DM1; $d_t^{2,c}$ denotes the transfer of cryptocurrency in the DM2; and $(d_t^{3,m}, d_t^{3,c})$ denote the transfers of fiat money and cryptocurrency, respectively, in the DM3.

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. Otherwise, if there is no match, then agents proceed to the next period with the same currency portfolios that they carry out of the centralized market.

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:

$$
\begin{aligned}
\text{In the DM1:} \quad & \max_{q_t^1, d_t^1} \quad u(q_t^1) + \beta W_{t+1}^b(m_t^{m,b} - d_t^{1,m}, m_t^{c,b}) \\
s.t. \quad & -\omega(q_t^1) + \beta W_{t+1}^s(m_t^{m,s} + d_t^{1,m}, m_t^{c,s}) \geq \beta W_{t+1}^s(m_t^{m,s}, m_t^{c,s}) \\
& d_t^{1,m} \leq m_t^{m,b}
\end{aligned} \tag{37}
$$

$$
\begin{aligned}
\text{In the DM2:} \quad & \max_{q_t^2, d_t^2} \quad u(q_t^2) + \beta W_{t+1}^b(m_t^{m,b}, m_t^{c,b} - d_t^{2,c}) \\
s.t. \quad & -\omega(q_t^2) + \beta W_{t+1}^s(m_t^{m,s}, m_t^{c,s} + d_t^{2,c}) \geq \beta W_{t+1}^s(m_t^{m,s}, m_t^{c,s}) \\
& d_t^{2,c} \leq m_t^{c,b}
\end{aligned} \tag{38}
$$

$$
\begin{aligned}
\text{In the DM3:} \quad & \max_{q_t^3, d_t^{3,m}, d_t^{3,c}} \quad u(q_t^3) + \beta W_{t+1}^b(m_t^{m,b} - d_t^{3,m}, m_t^{c,b} - d_t^{3,c}) \\
s.t. \quad & -\omega(q_t^3) + \beta W_{t+1}^s(m_t^{m,s} + d_t^{3,m}, m_t^{c,s} + d_t^{3,c}) \geq \beta W_{t+1}^s(m_t^{m,s}, m_t^{c,s}) \\
& d_t^{3,m} \leq m_t^{m,b}, d_t^{3,c} \leq m_t^{c,b}
\end{aligned} \tag{39}
$$

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

Substituting (33) and (34), problems (37)-(39) can be simplified as follows.

$$\text{In the DM1:} \quad \max_{q_t^1, d_t^{1,m}} \quad u(q_t^1) - \beta p_{t+1}^m d_t^{1,m}$$
$$s.t. \quad -\omega(q_t^1) + \beta p_{t+1}^m d_t^{1,m} \geq 0 \tag{40}$$
$$d_t^{1,m} \leq m_t^{m,b}$$

$$\text{In the DM2:} \quad \max_{q_t^2, d_t^{2,c}} \quad u(q_t^2) - \beta p_{t+1}^c (1-\pi) d_t^{2,c}$$
$$s.t. \quad -\omega(q_t^2) + \beta p_{t+1}^c (1-\pi) d_t^{2,c} \geq 0 \tag{41}$$
$$d_t^{2,c} \leq m_t^{c,b}$$

$$\text{In the DM3:} \quad \max_{q_t^3, d_t^{3,m}, d_t^{3,c}} \quad u(q_t^3) - \beta p_{t+1}^m d_t^{3,m} - \beta p_{t+1}^c (1-\pi) d_t^{3,c}$$
$$s.t. \quad -\omega(q_t^3) + \beta p_{t+1}^m d_t^{3,m} + \beta p_{t+1}^c (1-\pi) d_t^{3,c} \geq 0 \tag{42}$$
$$d_t^{3,m} \leq m_t^{m,b}, d_t^{3,c} \leq m_t^{c,b}$$

Similar to the cryptocurrency-only economy, the buyer's offer in each decentralized market is independent of the seller's currency portfolio, $(m_t^{m,s}, m_t^{c,s})$. Thus, the optimal offer in each match is such that seller's participation constraint holds with equality.

Under Assumptions 2.1, $q^* = \text{argmax}\,[u(q_t) - \omega(q_t)]$ is the traded amount that maximizes the trade surplus between a buyer and seller in each match. If a buyer can afford q^* using the currencies that are accepted as payment methods in that decentralized market, then the buyer would make enough payment to get q^*, i.e., $d_t^{1,m} = m_t^{m*},\ d_t^{2,c} = m_t^{c*},\ (d_t^{3,m}, d_t^{3,c}) = (\hat{m}_t^{m,b}, \hat{m}_t^{c,b})$ s.t. $\omega(q^*) = \beta(p_{t+1}^m \hat{m}_t^{m,b} + p_{t+1}^c (1-\pi)\hat{m}_t^{c,b})$. Otherwise, the buyer would spend all the currencies that can be used in that market to purchase the DM good. More specifically, in the DM1: $(d^{1,m} = m_t^{m,b}, q_t^1 = \omega^{-1}(\beta p_{t+1}^m m_t^{m,b}))$; in the DM2: $(d^{2,c} = m_t^{c,b}, q_t^2 = \omega^{-1}(\beta p_{t+1}^c (1-\pi) m_t^{c,b}))$; and in the DM3: $((d_t^{3,m}, d_t^{3,c}) = (m_t^{m,b}, m_t^{c,b}), q_t^3 = \omega^{-1}(\beta p_{t+1}^m m_t^{m,b} + \beta p_{t+1}^c (1-\pi) m_t^{c,b}))$, where $q_t^{DM} < q^*,\ \forall DM \in \{1,2,3\}$. Two currencies are perfect substitutes in the DM3. Solutions to (40)-(42) are summarized in the following Lemma.

Lemma 4.1. *Terms of Trade in Two-Currency Model*

i. In the DM 1 where only fiat money can be used, solutions to the terms of trade $(q_t^1, d_t^{1,m})$ are given by:

$$q_t^1(m_t^{m,b}) = \begin{cases} q^* & if \;\; m_t^{m,b} \geq m_t^{m*} \\ \hat{q}_t^1 & if \;\; m_t^{m,b} < m_t^{m*} \end{cases} \quad d_t^{1,m}(m_t^{m,b}) = \begin{cases} m_t^{m*} & if \;\; m_t^{m,b} \geq m_t^{m*} \\ m_t^{m,b} & if \;\; m_t^{m,b} < m_t^{m*} \end{cases} \tag{43}$$

ii. In the DM 2 where only cryptocurrency can be used, solutions to the terms of trade $(q_t^2, d_t^{2,c})$ are given by:

$$q_t^2(m_t^{c,b}) = \begin{cases} q^* & if \;\; m_t^{c,b} \geq m_t^{c*} \\ \hat{q}_t^2 & if \;\; m_t^{c,b} < m_t^{c*} \end{cases} \quad d_t^{2,c}(m_t^{c,b}) = \begin{cases} m_t^{c*} & if \;\; m_t^{c,b} \geq m_t^{c*} \\ m_t^{c,b} & if \;\; m_t^{c,b} < m_t^{c*} \end{cases} \tag{44}$$

iii. In the DM 3 where both currencies can be used, solutions to the terms of trade $(q_t^3, d_t^{3,m}, d_t^{3,c})$ are given by:

$$q_t^3(\mathbf{m}_t^b) = \begin{cases} q^* & if \quad \beta(p_{t+1}^m m_t^{m,b} + (1-\pi)p_{t+1}^c m_t^{c,b}) \geq \omega(q^*) \\ \hat{q}_t^3 & if \quad \beta(p_{t+1}^m m_t^{m,b} + (1-\pi)p_{t+1}^c m_t^{c,b}) < \omega(q^*) \end{cases} \tag{45}$$

$$(d_t^{3,m}(\mathbf{m}_t^b), d_t^{3,c}(\mathbf{m}_t^b)) = \begin{cases} (\hat{m}_t^{m,b}, \hat{m}_t^{c,b}) & if \quad \beta(p_{t+1}^m m_t^{m,b} + (1-\pi)p_{t+1}^c m_t^{c,b}) \geq \omega(q^*) \\ \quad s.t. \quad \omega(q^*) = \beta(p_{t+1}^m \hat{m}_t^{m,b} + p_{t+1}^c(1-\pi)\hat{m}_t^{c,b}) & \\ (m_t^{m,b}, m_t^{c,b}) & if \quad \beta(p_{t+1}^m m_t^{m,b} + (1-\pi)p_{t+1}^c m_t^{c,b}) < \omega(q^*) \end{cases}$$

where $q^* = argmax\,[u(q_t) - \omega(q_t)]$, $m_t^{m*} = \frac{\omega(q^*)}{\beta p_{t+1}^m}$, and $m_t^{c*} = \frac{\omega(q^*)}{\beta p_{t+1}^c(1-\pi)}$;
$\hat{q}_t^1 = \omega^{-1}(\beta p_{t+1}^m m_t^{m,b})$, $\hat{q}_t^2 = \omega^{-1}(\beta p_{t+1}^c(1-\pi)m_t^{c,b})$, $\hat{q}_t^3 = \omega^{-1}(\beta p_{t+1}^m m_t^{m,b} + \beta p_{t+1}^c(1-\pi)m_t^{c,b})$;
and $\hat{q}_t^{DM} < q^*$, $\forall DM \in \{1,2,3\}$.

Next, following Lemma 4.1, we can rewrite the DM value functions as follows.

$$V_t^b(m_t^{m,b}, m_t^{c,b}) = \beta(p_{t+1}^m m_t^{m,b} + (1-\pi)p_{t+1}^c m_t^{c,b} + W_{t+1}^b(0,0)) + \{\underbrace{\alpha_1\sigma[u(q_t^1(m_t^{m,b})) - \beta p_{t+1}^m d_t^{1,m}(m_t^{m,b})]}_{\text{a buyer's expected surplus in the DM1}}\}$$
$$+ \{\underbrace{\alpha_2\sigma[u(q_t^2(m_t^{c,b})) - \beta p_{t+1}^c(1-\pi)d_t^{2,c}(m_t^{c,b})]}_{\text{a buyer's expected surplus in the DM2}}\}$$
$$+ \{\underbrace{\alpha_3\sigma[u(q_t^3(\mathbf{m}_t^b)) - \beta p_{t+1}^m d_t^{3,m}(\mathbf{m}_t^b) - \beta p_{t+1}^c(1-\pi)d_t^{3,c}(\mathbf{m}_t^b)]}_{\text{a buyer's expected surplus in the DM3}}\}$$

$$V_t^s(m_t^{m,s}, m_t^{c,s}) = \beta(p_{t+1}^m m_t^{m,s} + (1-\pi)p_{t+1}^c m_t^{c,s} + W_{t+1}^s(0,0)) + \underbrace{0+0+0}_{\text{a seller's expected surplus in all DMs}}$$

Since buyers are the ones to make the take-it-or-leave-it offer, buyers take all the gains and sellers have no surplus from trades in any decentralized market.

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

Substituting the above DM value functions into (33)-(34), the optimal currency portfolios of a buyer and seller are given by the solutions to:

$$W_t^b(m_{t-1}^{m,b}, m_{t-1}^{c,b}) = \max_{m_t^{m,b}, m_t^{c,b} \in \mathbb{R}_+^2} -\underbrace{(p_t^m - \beta p_{t+1}^m)m_t^{m,b}}_{\text{cost of holding fiat money}} - \underbrace{(p_t^c - \beta(1-\pi)p_{t+1}^c)m_t^{c,b}}_{\text{cost of holding cryptocurrency}} \tag{46}$$
$$+ \underbrace{\alpha_1\sigma[u(q_t^1(m_t^{m,b})) - \beta p_{t+1}^m d_t^{1,m}(m_t^{m,b})]}_{\text{a buyer's expected surplus in DM1, } v_t^1} + \underbrace{\alpha_2\sigma[u(q_t^2(m_t^{c,b})) - \beta p_{t+1}^c(1-\pi)d_t^{2,c}(m_t^{c,b})]}_{\text{buyer's expected surplus in DM2, } v_t^2}$$
$$+ \underbrace{\alpha_3\sigma[u(q_t^3(m_t^{m,b}, m_t^{c,b})) - \beta p_{t+1}^m d_t^{3,m}(m_t^{m,b}, m_t^{c,b}) - \beta p_{t+1}^c(1-\pi)d_t^{3,c}(m_t^{m,b}, m_t^{c,b})]}_{\text{a buyer's expected surplus in DM3, } v_t^3}$$

$$W_t^s(m_{t-1}^{m,s}, m_{t-1}^{c,s}) = \max_{m_t^{m,s}, m_t^{c,s} \in \mathbb{R}_+^2} -\underbrace{(p_t^m - \beta p_{t+1}^m)m_t^{m,s}}_{\text{cost of holding fiat money}} - \underbrace{(p_t^c - \beta(1-\pi)p_{t+1}^c)m_t^{c,s}}_{\text{cost of holding cryptocurrency}}$$
$$+ \underbrace{0}_{\text{expected surplus in DM 1}} + \underbrace{0}_{\text{expected surplus in DM 2}} + \underbrace{0}_{\text{expected surplus in DM 3}} \tag{47}$$

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. From (46)-(47), cryptocurrency is costly to carry when $p_t^c > \beta p_{t+1}^c(1-\pi)$, 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 first-order conditions of (46)-(47) with respect to $[m^{m,j}]$ and $[m^{c,j}]$, $j \in \{b, s\}$, respectively.

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

$$[m_t^{m,b}] \quad \frac{p_t^m}{\beta p_{t+1}^m} - 1 \geq \alpha_1 \sigma L(p_{t+1}^m m_t^{m,b}) + \alpha_3 \sigma L(p_{t+1}^m m_t^{m,b} + (1-\pi) p_{t+1}^c m_t^{c,b})$$
$$\text{“}=\text{”} \ \textit{if} \quad m_t^{m,b} > 0 \tag{48}$$

$$[m_t^{c,b}] \quad \frac{p_t^c}{\beta p_{t+1}^c (1-\pi)} - 1 \geq \alpha_2 \sigma L(p_{t+1}^c (1-\pi) m_t^{c,b}) + \alpha_3 \sigma L(p_{t+1}^m m_t^{m,b} + (1-\pi) p_{t+1}^c m_t^{c,b})$$
$$\text{“}=\text{”} \ \textit{if} \quad m_t^{c,b} > 0 \tag{49}$$

$$[m_t^{m,s}] \quad -p_t^m + \beta p_{t+1}^m \leq 0$$
$$\text{“}=\text{”} \quad \textit{if} \quad m_t^{m,s} > 0 \tag{50}$$

$$[m_t^{c,s}] \quad -p_t^c + \beta p_{t+1}^c (1-\pi) \leq 0$$
$$\text{“}=\text{”} \quad \textit{if} \quad m_t^{c,s} > 0 \tag{51}$$

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

The term $L(\cdot)$ represents the liquidity premium, which captures the marginal payoff that an agent can get from liquid assets that are used to purchase more outputs in a decentralized market. Similar to Lemma 2.4, $L(\cdot) = 0$ when buyers can make enough payment to purchase q^* in a decentralized meeting, whereas $L(\cdot) > 0$ when buyers can not afford q^*.

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. From Lemma 4.2, there is no solution to $m_t^{c,j}$ when $\frac{p_t^c}{p_{t+1}^c} < \beta(1-\pi)$, and there is no solution to $m_t^{m,j}$ when $\frac{p_t^m}{p_{t+1}^m} < \beta, \ \forall j \in \{b, s\}$. 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. From (50)-(51), a seller will not carry any unit of fiat money or cryptocurrency out of the centralized market if that currency is costly to carry.

5. Equilibrium

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

Definition 4. *Given γ, an equilibrium is a set of decision rules in the centralized market $\{x_t^b, \mathbf{m}_t^b, x_t^s, \mathbf{m}_t^s, x_t^i, m_t^{m,i}, \delta_t^i\}_{t=0}^{\infty}$, the terms of trade in each decentralized market $\{(q_t^1, d_t^{1,m}), (q_t^2, d_t^{2,c}), (q_t^3, d_t^{3,m}, d_t^{3,c})\}_{t=0}^{\infty}$, 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 (31)-(32) and (35)-(36); $\{x_t^i, \delta_t^i, m_t^{m,i}\}$ solve problem (27); $\{(q_t^1, d_t^{1,m}), (q_t^2, d_t^{2,c}), (q_t^3, d_t^{3,m}, d_t^{3,c})\}$ solve problems (40)-(42); as well as market clearing for centralized good, fiat money, and cryptocurrency, and cryptocurrency law of motion 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 characterize the stationary equilibrium in the two-currency economy. My focus is on examining whether cryptocurrency – an asset that is costly to produced – can coexist with fiat money – an asset that is costless to produce – in the economy.

Assume 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 $\mu > -\pi$. 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.

$$i_m \ \geq \ \alpha_1 \sigma L(\frac{z_m}{\gamma}) + \alpha_3 \sigma L(\frac{z_m}{\gamma} + \frac{(1-\pi)z_c}{1+\mu}) \qquad \text{“}=\text{”} \text{ if } \ z_m > 0 \tag{52}$$

$$i_c \ \geq \ \alpha_2 \sigma L(\frac{(1-\pi)z_c}{1+\mu}) + \alpha_3 \sigma L(\frac{z_m}{\gamma} + \frac{(1-\pi)z_c}{1+\mu}) \qquad \text{“}=\text{”} \text{ if } \ z_c > 0 \tag{53}$$

where $i_m = \frac{p_t^m}{\beta p_{t+1}^m} - 1$ and $i_c = \frac{p_t^c}{\beta p_{t+1}^c (1-\pi)} - 1$ denote the cost of carrying fiat money and cryptocurrency, respectively, which depend on the rate of return, time preference, and the currency depreciation rate.[23] According to (52)-(53), 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 fiat money supply.

[23]The term $1 + i_m$ can be interpreted as the interest rate on an illiquid nominal bond dominated in fiat money (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 the growth rules on two currencies, γ, μ, and the parameters 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. That is, $i_m \geq \alpha_1\sigma L(0) + \alpha_3\sigma L(0)$ and $i_c \geq \alpha_2\sigma L(0) + \alpha_3\sigma L(0)$. Accordingly, given the parameters of the model and the growth rule of each currency, 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:

$$\frac{\tilde{\gamma}}{\beta} - 1 = \alpha_1\sigma L(0) + \alpha_3\sigma L(0) \tag{54}$$

$$\frac{1+\tilde{\mu}}{\beta(1-\pi)} - 1 = \alpha_2\sigma L(0) + \alpha_3\sigma L(0) \tag{55}$$

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 α_2, the size of the markets in which sellers only accept cryptocurrency for transactions, is too small, or when the cryptocurrency depreciation rate, π, 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 (54) and $\bar{\mu}$ is given by:

$$\frac{1+\bar{\mu}}{\beta(1-\pi)} - 1 = \alpha_2\sigma L(0) + \frac{\alpha_3}{\alpha_1+\alpha_3}\left(\frac{\gamma}{\beta} - 1\right) \tag{56}$$

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 $1-\pi < 1+\mu < 1+\tilde{\mu}$, where $1+\tilde{\mu}$ is from (55) and $\bar{\gamma}$ is given by:

$$\frac{\bar{\gamma}}{\beta} - 1 = \alpha_1\sigma L(0) + \frac{\alpha_3}{\alpha_2+\alpha_3}\left(\frac{1+\mu}{\beta(1-\pi)} - 1\right) \tag{57}$$

Lastly, a stationary equilibrium in which both cryptocurrency and fiat money are valued, i.e., $z_m > 0$ and $z_c > 0$, exists so long as $\beta < \gamma < \bar{\gamma}$ and $1-\pi < 1+\mu < 1+\bar{\mu}$, where $\bar{\gamma}$ and $\bar{\mu}$ are given by (57) and (56), respectively.

5.1. Coexistence

Next, I characterize the stationary equilibrium in which both cryptocurrency and fiat money are valued in the economy.

Proposition 3. *Given γ and $\alpha_{DM} \in (0,1)\ \forall DM \in \{1,2,3\}$, 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 stock of cryptocurrency is constant and that of fiat money grows at a constant rate $\gamma - 1$, so long as $\beta < \gamma < \bar{\gamma} \equiv \beta\alpha_1\sigma L(0) + \frac{\alpha_3}{\alpha_2+\alpha_3}(\frac{1}{1-\pi} - \beta) + \beta$ and $0 < \hat{\mu} \equiv (\alpha_2\sigma L(0)+1)\beta(1-\pi) - 1$. The equilibrium outcomes are characterized by:*

$$\frac{\gamma-\beta}{\sigma\beta} = \alpha_1[\frac{u' \circ \omega^{-1}(\beta\frac{z_m}{\gamma})}{\omega' \circ \omega^{-1}(\beta\frac{z_m}{\gamma})} - 1] + \alpha_3[\frac{u' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\pi)))}{\omega' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\pi)))} - 1] \tag{58}$$

$$\frac{1-\beta(1-\pi)}{\sigma\beta(1-\pi)} = \alpha_2[\frac{u' \circ \omega^{-1}(\beta z_c(1-\pi))}{\omega' \circ \omega^{-1}(\beta z_c(1-\pi))} - 1] + \alpha_3[\frac{u' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\pi)))}{\omega' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\pi)))} - 1] \tag{59}$$

$$p_c^{ss} = (D + 2B\pi)M_c^{ss} \tag{60}$$

$$q_1^{ss} = \omega^{-1}(\beta\frac{z_m}{\gamma}) \tag{61}$$

$$q_2^{ss} = \omega^{-1}(\beta z_c(1-\pi)) \tag{62}$$

$$q_3^{ss} = \omega^{-1}(\beta\frac{z_m}{\gamma} + \beta z_c(1-\pi)) \tag{63}$$

$$\Delta^{ss} = \pi M_c^{ss} \tag{64}$$

Following Propositions 1 and 2, the stock of cryptocurrency must be constant in the stationary equilibrium in which cryptocurrency is valued. Then 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 (58)-(64) so long as $\beta < \gamma < \bar{\gamma}$ and $0 < \hat{\mu}$, where $\bar{\gamma}$ is obtained from (57) with $\mu = 0$, and $\hat{\mu}$ is given by (56) with $\gamma = \beta$.

Different from what happens in the 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 two currencies have different degrees of acceptability in decentralized markets. Since each currency is essential in some meetings, agents will hold both currencies in order to to smooth their consumption in all decentralized meetings, even if one is issued at a higher growth rate, and thus, 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.

In addition, different from the equilibrium with coexistence in the models of private and fiat monies, in which private money is exogenously supplied according to a growth rule (e.g., Zhu and Hendry (2019)), I show that in the economy where the aggregate cryptocurrency supply is endogenously determined, the stock of cryptocurrency must be constant in equilibrium.[24]

Moreover, from Proposition 3, the real balances of fiat money, z_m, and cryptocurrency, z_c, are interdependent. Therefore, the government monetary policy, γ, can affect the value of cryptocurrency, and hence, affect the quantity of DM good traded with cryptocurrency in the DM2, q_2^{ss}.

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 markets; $2)$ when cryptocurrency has an inherent advantage relative to fiat money; $3)$ when fiat money has an inherent advantage relative to cryptocurrency.

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 $\alpha_3 = 0$. In this case, agents can only trade with fiat money in the DM1 and only trade with cryptocurrency in the DM2. Then (52)-(53) can be expressed as follows:

$$i_m \geq \alpha_1 \sigma L(\frac{z_m}{\gamma}) \qquad \text{“}=\text{” if } z_m > 0 \tag{65}$$

$$i_c \geq \alpha_2 \sigma L(\frac{z_c(1-\pi)}{1+\mu}) \qquad \text{“}=\text{” if } z_c > 0 \tag{66}$$

To be valued and circulating in the economy, the cost of carrying an additional unit of the currency must equal the expected payoff of using it in decentralized meetings.

[24] In Appendix C, I present a version of the two-currency economy where both cryptocurrency and fiat money are exogenously supplied. In that model, there exists an equilibrium in which two currencies are valued and in which the stock of cryptocurrency grows at a constant rate. Thus, different from the model where cryptocurrency is costly to produce and its aggregate supply is endogenously determined, the model with exogenously supplied cryptocurrency cannot have an analog of the equilibrium in which the stock of cryptocurrency must remain constant.

Proposition 4. *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 stock of cryptocurrency is constant and that of fiat money grows at a constant rate $\gamma - 1$, so long as $\beta < \gamma < \bar{\gamma} \equiv \beta\alpha_1\sigma L(0) + \beta$ and $0 < \bar{\mu} \equiv (\alpha_2\sigma L(0) + 1)\beta(1-\pi) - 1$. The equilibrium outcomes are characterized by:*

$$\frac{\gamma - \beta}{\sigma\beta} = \alpha_1[\frac{u' \circ \omega^{-1}(\beta\frac{z_m}{\gamma})}{\omega' \circ \omega^{-1}(\beta\frac{z_m}{\gamma})} - 1] \tag{67}$$

$$\frac{1 - \beta(1-\pi)}{\sigma\beta(1-\pi)} = \alpha_2[\frac{u' \circ \omega^{-1}(\beta z_c(1-\pi))}{\omega' \circ \omega^{-1}(\beta z_c(1-\pi))} - 1] \tag{68}$$

$$p_c^{ss} = (D + 2B\pi)M_c^{ss} \tag{69}$$

$$q_1^{ss} = \omega^{-1}(\beta\frac{z_m}{\gamma}) \tag{70}$$

$$q_2^{ss} = \omega^{-1}(\beta z_c(1-\pi)) \tag{71}$$

$$\Delta^{ss} = \pi M_c^{ss} \tag{72}$$

The terms $\bar{\gamma}$ and $\bar{\mu}$ are obtained from (56)-(57) with $\alpha_3 = 0$. Under Assumptions 2.1 and 2.2 and given the fundamentals and parameters of the model, there is a unique set of equilibrium outcomes that satisfy (67)-(72).

Since each currency is essential in a decentralized market, agents will hold both currencies to smooth consumption in two decentralized markets, so long as neither currency is too costly to carry. Thus, similar to Proposition 3, cryptocurrency and fiat money can coexist in the economy with different rates of return.

Unlike Proposition 3, there is a dichotomy between two currencies' sectors in the economy where $\alpha_3 = 0$, since there is no interaction between the DM1 and DM2. Specifically, the real balances of cryptocurrency and fiat money, z_c and z_m, are independent, and the quantity of the DM good traded with cryptocurrency in the DM2, q_2^{ss}, is determined independently from that traded with fiat money in the DM1, q_1^{ss}. Therefore, the government monetary policy, γ, has no effects on the cryptocurrency use. The equilibrium outcomes of cryptocurrency only depend on the fundamentals of the economy, such as preferences, technologies, and trading frictions.

6.2. Inherent Advantage to One Currency

Next, 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 since agents can trade with cryptocurrency everywhere (in both the DM2 and DM3) but can only trade with fiat money in the DM3. Then (52)-(53) can be expressed as follows.

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

$$i_c \ \geq\ \alpha_2 \sigma L(\frac{z_c(1-\pi)}{1+\mu}) + \alpha_3 \sigma L(\frac{z_m}{\gamma} + \frac{z_c(1-\pi)}{1+\mu}) \qquad \text{“}=\text{”} \text{ if } \ z_c > 0 \tag{74}$$

Agents compare the cost and benefit of holding the currency when they choose currency portfolios. 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 5. *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 stock of cryptocurrency is constant and that of fiat money grows at a constant rate $\gamma - 1$, so long as $\beta < \gamma < \bar{\gamma} \equiv \alpha_3(\frac{1}{1-\pi} - \beta) + \beta$ and $0 < \hat{\mu} \equiv (\alpha_2 \sigma L(0) + 1)\beta(1-\pi) - 1$. The equilibrium outcomes are characterized by:*

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

$$\frac{1 - \beta(1-\pi)}{\sigma\beta(1-\pi)} = \alpha_2[\frac{u' \circ \omega^{-1}(\beta z_c(1-\pi))}{\omega' \circ \omega^{-1}(\beta z_c(1-\pi))} - 1] + \frac{\gamma - \beta}{\sigma\beta} \tag{76}$$

$$p_c^{ss} = (D + 2B\pi)M_c^{ss} \tag{77}$$

$$q_2^{ss} = \omega^{-1}(\beta z_c(1-\pi)) \tag{78}$$

$$q_3^{ss} = \omega^{-1}(\beta\frac{z_m}{\gamma} + \beta z_c(1-\pi)) \tag{79}$$

$$\Delta^{ss} = \pi M_c^{ss} \tag{80}$$

The term $\bar{\gamma}$ is obtained from (57) with $\alpha_1 = \mu = 0$, and $\hat{\mu}$ is obtained from (56) given $\gamma \in (\beta, \bar{\gamma})$. Under Assumptions 2.1 and 2.2, and given the forms of $u(\cdot), \omega(\cdot)$, and parameters of the economy, there exists a unique set of equilibrium outcomes that satisfy (75)-(80).

Intuitively, since cryptocurrency can be used as a payment method everywhere, agents will carry cryptocurrency to facilitate all kinds of transactions in decentralized markets, as long as cryptocurrency 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 cryptocurrency depreciation rate and the market size where fiat money can be used. Otherwise, when $\gamma \geq \bar{\gamma}$, 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 (in both the DM1 and DM3), whereas cryptocurrency is only accepted in the DM3. Then (52)-(53) can be expressed as follows.

$$i_m \ \geq \ \alpha_1 \sigma L(\frac{z_m}{\gamma}) + \alpha_3 \sigma L(\frac{z_m}{\gamma} + \frac{z_c(1-\pi)}{1+\mu}) \qquad \text{“}=\text{”} \text{ if } \ z_m > 0 \tag{81}$$

$$i_c \ \geq \ \alpha_3 \sigma L(\frac{z_m}{\gamma} + \frac{z_c(1-\pi)}{1+\mu}) \qquad \text{“}=\text{”} \text{ if } \ z_c > 0 \tag{82}$$

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

Proposition 6. *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 stock of cryptocurrency is constant and that of fiat money grows at a constant rate $\gamma - 1$, so long as $\frac{1}{\alpha_3}(\frac{1}{1-\pi} - \beta) + \beta \equiv \hat{\gamma} < \gamma < \bar{\gamma} \equiv \beta\alpha_1\sigma L(0) + \frac{1}{1-\pi}$. Gresham's law does not hold. The equilibrium outcomes are characterized by:*

$$\frac{\gamma - \beta}{\sigma\beta} = \alpha_1[\frac{u' \circ \omega^{-1}(\beta\frac{z_m}{\gamma})}{\omega' \circ \omega^{-1}(\beta\frac{z_m}{\gamma})} - 1] + \frac{1-\beta(1-\pi)}{\sigma\beta(1-\pi)} \tag{83}$$

$$\frac{1-\beta(1-\pi)}{\sigma\beta(1-\pi)} = \alpha_3[\frac{u' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\pi)))}{\omega' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\pi)))} - 1] \tag{84}$$

$$p_c^{ss} = (D + 2B\pi)M_c^{ss} \tag{85}$$

$$q_1^{ss} = \omega^{-1}(\beta\frac{z_m^{ss}}{\gamma}) \tag{86}$$

$$q_3^{ss} = \omega^{-1}(\beta\frac{z_m^{ss}}{\gamma} + \beta z_c(1-\pi)) \tag{87}$$

$$\Delta^{ss} = \pi M_c^{ss} \tag{88}$$

Under Assumptions 2.1 and 2.2, there is a unique set of equilibrium outcomes that satisfy (83)-(88), given the forms of $u(\cdot), \omega(\cdot)$, and parameters of the economy.

Cryptocurrency and fiat money can coexist in the economy when fiat money is issued at a growth rate higher than a certain level, $\hat{\gamma}$, i.e., has a high inflation rate in equilibrium. Intuitively, since fiat money can be used as a payment method everywhere, agents will carry fiat money to facilitate all kinds of transactions in decentralized markets, as long as fiat money is not too costly to hold. Agents will carry cryptocurrency as well when the rate of return on cryptocurrency is much higher than that on fiat money.

Proposition 6 shows that, Gresham's Law —"Bad money drives out good money"— does not hold in this economy, since 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 fiat and commodity monies. For example, Velde et al. (1999) shows that Gresham's Law holds in an economy with heavy and light coins, and Camera et al. (2004) produces the highest velocity for the safe money relative to risky money, where Gresham's Law was 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 and 6, 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 competition with cryptocurrency restricts the inflation rate of fiat money and thus restricts the government's ability to over-issue 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. Since cryptocurrency is costly to produce, banning cryptocurrency will avoid the resource cost on production, i.e., $c(\delta, M^c)$. However, since sellers in the DM2 only accept cryptocurrency as the payment method, banning cryptocurrency will make agents unable to trade in the DM2 and only able to trade with fiat money in the DM3. Thus, banning cryp-

tocurrency will result in welfare loss from no trade surplus in the DM2, i.e., $-\alpha_2[u(q_2) - \omega(q_2)]$, where $q_2 = \omega^{-1}(\beta z_c(1-\pi))$, and result in welfare changes from trade surplus in the DM3, i.e., $\alpha_3[u(q_3^{'}) - \omega(q_3^{'})] - \alpha_3[u(q_3) - \omega(q_3)]$, where $q_3^{'} = \omega^{-1}(\beta \frac{z_m}{\gamma})$ and $q_3 = \omega^{-1}(\beta \frac{z_m}{\gamma} + \beta z_c(1-\pi))$.

In addition, the competition with cryptocurrency restricts the government's ability to over-issue fiat money. If the government tends to over-issue money, banning cryptocurrency would worsen the welfare of the economy since there would be welfare loss in all decentralized markets: no trade surplus in the DM2 and less trade surplus in the DM1 and DM3 from consuming less using fiat money. However, if the government can maintain sufficient 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 in the markets where fiat money is used, which would outweigh the welfare loss from no trade surplus in the DM2.[25] Efficient allocations in the DM1 and DM3 can be achieved when the monetary policy follows the Friedman rule if cryptocurrency is banned.

7. Conclusion

This paper studies the role of cryptocurrency - private money that is costly to produce - as a medium of exchange, and analyzes the coexistence of cryptocurrency and fiat money, which is 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 using the technology, into the economy. The cryptocurrency production cost increases in both the amount of newly produced units and the existing stock. Unlike fiat money models, there is no equilibrium in which the growth rate of cryptocurrency supply is positive. In the equilibrium in which cryptocurrency is valued and produced, the stock of cryptocurrency must remain constant.

I then develop a currency competition model between cryptocurrency and fiat money, in which 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

[25] Here 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.

more acceptable and costless to produce, when appropriate monetary policy is implemented. Furthermore, the competition with cryptocurrency restricts the government's ability to over-issue fiat money. The policy implication of my analysis is that, if the government tends to over-issue money, then banning cryptocurrency would worsen the welfare of the economy. But if the government can maintain sufficiently low inflation and the cryptocurrency's degree of acceptability in decentralized meetings is small, then banning cryptocurrency would be welfare-enhancing.

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. Can currency competition work? *Journal of Monetary Economics*, 106:1–15, 2019.

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.

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 (4), a buyer's optimal cryptocurrency holdings satisfy:

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

From (12): $V_t^b(m_t^b) = \beta(p_{t+1}(1-\pi)m_t^b + W_{t+1}^b(0)) + v_t(m_t^b)$, where

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

Then we obtain:

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

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.

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

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 $\forall m_t^b < m_t^*$. Because of the concavity of $V(\cdot)$, there is a unique $m_t^b < m_t^*$ solving the problem (A.1), which is expressed as (18) following (A.2).

□

[Proof of Lemma 2.6]

Proof. Under Assumption 2.2, taking the first-order condition of (20) with respect to $[\delta_t^i]$, we obtain $p_t = DM_{t-1} + 2B\delta_t^i$. Therefore, $\delta_t^i = \max[0, \frac{p_t - DM_{t-1}}{2B}]$.

□

[Proof of Proposition 1]

Proof. In stationary equilibrium, $p_t M_t = p_{t+1} M_{t+1} = z^{ss}$. When the stock of cryptocurrency is constant, from cryptocurrency law of motion, $\Delta^{ss} = \pi M^{ss}$. Combining it with the aggregate production (22), we obtain (24). Next, following Lemmas 2.4 and 2.5, the aggregate demand of cryptocurrency, M^d, satisfies:

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

Under Assumptions 2.1 and 2.2, and given the forms of $u(\cdot), \omega(\cdot)$, and parameters of the model, there exists a unique value of p^{ss} and M^{ss} that satisfy both (A.3) and (24) with $M^{ss} = M^d$. Therefore, there is a unique value of $z^{ss} = p^{ss} M^{ss}$ that solves (23), and following Lemma 2.2, there is a unique q^{ss} that solves (25). By construction, the above results constitute a unique monetary stationary equilibrium, in which the stock of cryptocurrency is constant.

□

[Proof of Proposition 2]

Proof. Suppose the stock of cryptocurrency grows at a constant rate, i.e., $M_{t+1} = (1+\mu)M_t$, where $\mu > -\pi$ and $\mu \neq 0$. From (1) and (22), the aggregate production of cryptocurrency satisfies $\Delta_{t+1} = \frac{p_{t+1} - DM_t}{2B}$ and $\Delta_{t+1} = (\mu + \pi)M_t$. Then we have:

$$p_{t+1} = [2B(\mu + \pi) + D]M_t \tag{A.4}$$

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

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

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 over time, which contradicts to the assumption that the stock of cryptocurrency grows at a constant rate.

□

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

This section provides a special case to the cryptocurrency-only economy, where $M_{t+1} = (1+\mu)M_t$ and $\mu = -\pi$.

Proposition A.1. *Under Assumption 2.1, there exists a unique monetary stationary equilibrium, in which the stock of cryptocurrency shrinks at the depreciation rate s.t.* $M_{t+1} = (1-\pi)M_t$. *The equilibrium outcomes are characterized by:*

$$\frac{1-\beta}{\sigma\beta} = [\frac{u' \circ \omega^{-1}(\beta z^{ss})}{\omega' \circ \omega^{-1}(\beta z^{ss})} - 1] \tag{A.6}$$

$$q^{ss} = \omega^{-1}(\beta z^{ss}) \tag{A.7}$$

[Proof of Proposition A.1]

Proof. When the stock of cryptocurrency shrinks at the depreciation rate, i.e., $\mu = -\pi$, following (1), $\Delta_t = 0 \ \forall t$. That is, there is no production of cryptocurrency. In stationary equilibrium, $p_t M_t = p_{t+1} M_{t+1} = z^{ss}$. Following Lemmas 2.4 and 2.5, the real balance of cryptocurrency z^{ss} satisfies (A.6). Under Assumption 2.1, there exists a unique $z^{ss} > 0$ that solves (A.6). Next, following Lemma 2.2, the consumption of the DM good $q^{ss} < q^*$ can be uniquely determined by (A.7). By construction, the above results constitute a unique stationary equilibrium in which the stock of cryptocurrency shrinks at the depreciation rate. In that equilibrium, there is no production of cryptocurrency, $\Delta = 0$.

□

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

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

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

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

□

[Proof of Proposition 3]

Proof. From Propositions 1 and 2, the stock of cryptocurrency remains constant in the equilibrium in which cryptocurrency is valued. When $M^m_{t+1} = \gamma M^m_t$ and $M^c_{t+1} = (1+\mu)M^c_t$ with $\mu = 0$, 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 $\bar{\gamma} = \beta\alpha_1\sigma L(0) + \frac{\alpha_3}{\alpha_2+\alpha_3}(\frac{1}{1-\pi} - \beta) + \beta$ is obtained from (57) by replacing $\mu = 0$, and $\hat{\mu} = \beta(1-\pi)\{\alpha_2\sigma L(0) + 1\} - 1$ is obtained from (56), given $\gamma \in (\beta, \bar{\gamma})$.

In stationary equilibrium, $p^k_t M^k_t = p^k_{t+1}M^k_{t+1}, k \in \{m, c\}$. From (1) and (22), the aggregate production of cryptocurrency satisfies $\Delta^{ss} = \frac{p^{ss}_c - DM^{ss}_c}{2B}$ and $\Delta^{ss} = \pi M^{ss}_c$, which implies (60). From (52)-(53), the real balances of two currencies, z^{ss}_m and $z^{ss}_c = p^{ss}_c M^{ss}_c$, satisfy (58)-(59). Following Lemma 4.1, the steady state consumption of the DM good in each decentralized market satisfies (61)-(63). Given the functional forms and parameters of the model, the equilibrium outcomes can be jointly determined by (58)-(64), under Assumptions 2.1 and 2.2. By construction, the above results constitute a stationary equilibrium in which both fiat money and cryptocurrency are valued.

□

[Proof of Proposition 4]

Proof. Everything follows the Proof of Proposition 3 by replacing $\alpha_3 = 0$. Then, under Assumptions 2.1 and 2.2, a set of equilibrium outcomes can be uniquely determined using (67)-(72), given the functional forms and parameters of the model.

□

[Proof of Proposition 5]

Proof. Everything follows the Proof of Proposition 3 by replacing $\alpha_1 = 0$. Similarly, the equilibrium outcomes can be uniquely determined by (75)-(80), given the functional forms $u(\cdot), \omega(\cdot)$, and parameters of the model, under Assumptions 2.1 and 2.2.

□

[Proof of Proposition 6]

Proof. From Propositions 1 and 2, the stock of cryptocurrency remains constant in the equilibrium in which cryptocurrency is valued. When $M_{t+1}^m = \gamma M_t^m$ and $M_{t+1}^c = (1+\mu)M_t^c$ with $\mu = 0$, a stationary equilibrium in which $z_m > 0$ and $z_c > 0$ exists, so long as $\hat{\gamma} \leq \gamma < \bar{\gamma}$, where $\bar{\gamma} = \beta\alpha_1\sigma L(0) + \frac{1}{1-\pi}$ is obtained from (57) with $\mu = \alpha_2 = 0$ and $\hat{\gamma} = \frac{1}{\alpha_3}(\frac{1}{1-\pi} - \beta) + \beta$ is obtained from (56) with $\bar{\mu} > 0$. Then, following the Proof of Proposition 3 by replacing $\alpha_2 = 0$, under Assumptions 2.1 and 2.2, there exists a unique set of equilibrium outcomes that satisfy (83)-(88). □

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 amount of cryptocurrency the same. Therefore, 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 equilibrium in which the growth rate of cryptocurrency stock is positive. However, different from the model with currency loss, in the monetary stationary equilibrium in which the stock of cryptocurrency is constant, there is no production of cryptocurrency, i.e., $\Delta_t = 0 \ \forall t$. In this equilibrium, the cryptocurrency production will stop, and the only units of cryptocurrency 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_{t-1}^b and m_{t-1}^s units of cryptocurrency from the last period, respectively. A fraction of the buyer's cryptocurrency holdings, πm_{t-1}^b, is thieved, and meanwhile, the seller gets these thieved cryptocurrency units. In the centralized market, the buyer and seller choose their net consumption of the CM good and cryptocurrency holdings to bring forward to the decentralized market. Then the value functions in the centralized market become:

$$W_t^b(m_{t-1}^b) = \max_{x_t^b, m_t^b} \quad x_t^b + V_t^b(m_t^b), \qquad s.t. \qquad x_t^b + p_t m_t^b = p_t(1-\pi)m_{t-1}^b$$
$$W_t^s(m_{t-1}^s) = \max_{x_t^s, m_t^s} \quad x_t^s + V_t^s(m_t^s), \qquad s.t. \qquad x_t^s + p_t m_t^s = p_t(m_{t-1}^s + \pi m_{t-1}^b)$$

The above CM value functions can be rearranged as:

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

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

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 (7)-(8). 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, (q_t, d_t). Following (B.2)-(B.3), the terms of trade are given by the solution to the following problem.

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

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

Then the DM value functions can be expressed as:

$$V_t^b(m_t^b) = \beta(p_{t+1}(1-\pi)m_t^b + W_{t+1}^b(0)) + \underbrace{\sigma[u(q_t(m_t^b)) - (1-\pi)\omega(q_t(m_t^b))]}_{\text{a buyer's expected surplus in the DM, } v_t(m_t^b)} \tag{B.6}$$

$$V_t^s(m_t^s) = \beta(p_{t+1}(m_t^s + \pi m_t^b) + W_{t+1}^s(0)) + \underbrace{0}_{\text{a seller's expected surplus in the DM}} \tag{B.7}$$

Next, the optimal cryptocurrency holdings of a buyer and seller are given by the solutions to:

$$W_t^b(m_{t-1}^b) = \max_{m_t^b \in \mathbb{R}_+} - \underbrace{(p_t - p_{t+1}\beta(1-\pi))m_t^b}_{\text{the cost of carrying money to next period}} + \underbrace{\sigma[u(q_t(m_t^b)) - (1-\pi)\omega(q_t(m_t^b))]}_{\text{the expected surplus in the DM} = v_t(m_t^b)} \quad \text{(B.8)}$$

$$W_t^s(m_{t-1}^s) = \max_{m_t^s \in \mathbb{R}_+} - \underbrace{(p_t - p_{t+1}\beta)m_t^s}_{\text{the cost of carrying money to next period}} + \underbrace{0}_{\text{the expected surplus in the DM}} \quad \text{(B.9)}$$

For the buyer, cryptocurrency costly to carry when $\frac{p_t}{p_{t+1}} > \beta(1-\pi)$, whereas for the seller, it is costly to carry when $\frac{p_t}{p_{t+1}} > \beta$. Taking the first-order conditions of (B.8) and (B.9) with respect to m_t^b and m_t^s, respectively, the optimal cryptocurrency holdings of a typical buyer and seller satisfy:

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

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

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

When cryptocurrency is costly for buyers to carry, i.e., $\frac{p_t}{p_{t+1}} > \beta(1-\pi)$, 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. Then the aggregate new cryptocurrency supplied in period t, Δ_t, satisfies (22).

B.3. **Stationary Equilibrium**

The equilibrium definitions are the same as in Section 3, except for cryptocurrency law of motion that becomes (B.1). Next, I characterize the stationary equilibrium of the model with currency theft. Suppose the stock of cryptocurrency grows at a constant rate, i.e., $M_{t+1} = (1+\mu)M_t$. Then from (B.1), $\Delta_t = \mu M_{t-1}$. Since Δ_t cannot be negative, there is no solution to equilibrium when $\mu < 0$, and no cryptocurrency is produced when $\mu = 0$.

B.3.1. ***Constant Cryptocurrency Stock***

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

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

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

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

[Proof of Proposition B.1]

Proof. When the stock of cryptocurrency is constant, from (B.1), $\Delta_t = 0$. In stationary equilibrium, $p_t M_t = p_{t+1} M_{t+1} = z^{ss}$. 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 monetary stationary equilibrium, in which the stock of cryptocurrency is constant and no cryptocurrency is produced.

□

B.3.2. ***Time-Varying Cryptocurrency Stock***

Next, I examine the stationary equilibrium in which the stock of cryptocurrency grows at a constant rate, i.e., $\mu > 0$. Then $\Delta_t = \mu M_{t-1}\ \forall t$.

Proposition B.2. *Under Assumptions 2.1 and 2.2, there does not exist a monetary stationary equilibrium in which the stock of cryptocurrency grows at a constant rate.*

[Proof of Proposition B.2]

Proof. Suppose the stock of cryptocurrency grows at a constant rate, i.e., $\mu > 0$. From (B.1) and (22), the aggregate production of cryptocurrency satisfies $\Delta_{t+1} = \frac{p_{t+1} - D M_t}{2B}$ and $\Delta_{t+1} = \mu M_t$. Combining these two conditions, we obtain:

$$p_{t+1} = (2B\mu + D) M_t \tag{B.15}$$

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

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

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 over time, which contradicts to the assumption that the stock of cryptocurrency grows at a constant rate.

□

Appendix C. Exogenously Supplied Cryptocurrency

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

$$M_t^c = M_{t-1}^c + \underbrace{\Delta_t}_{\text{Newly produced}} - \underbrace{\pi M_{t-1}^c}_{\text{Depreciation}} = (1+\epsilon-\pi)M_{t-1}^c \tag{C.1}$$

I show that, there exists a stationary equilibrium in which both currencies are valued and in which the stock of cryptocurrency grows at a constant rate. This is different from the two-currency model with endogenously produced cryptocurrency in the main text, in which the stock of cryptocurrency must remain constant in equilibrium.

C.1. Buyers and Sellers

The problems faced by a typical buyer and seller are similar as in the two-currency economy described in Section 4. The only difference is that agents receive the new cryptocurrency supply in the form of lump-sum transfers during the first sub-period, i.e., $T_t^c = p_t^c \epsilon M_{t-1}^c$, expressed in terms of the CM good.

In the centralized market, agents choose the net consumption of the CM good and currency portfolios to bring forward to the next sub-period. The CM value functions are:

$$W_t^b(\mathbf{m_{t-1}^b}) = p_t^m m_{t-1}^{m,b} + (1-\pi)p_t^c m_{t-1}^{c,b} \underbrace{+T_t^m + T_t^c + \max_{\mathbf{m_t^b} \in \mathbb{R}_+^2} -\mathbf{p_t}\mathbf{m_t^b} + V_t^b(\mathbf{m_t^b})}_{W_t^b(0,0)} \tag{C.2}$$

$$W_t^s(\mathbf{m_{t-1}^s}) = p_t^m m_{t-1}^{m,s} + (1-\pi)p_t^c m_{t-1}^{c,s} \underbrace{+T_t^c + \max_{\mathbf{m_t^s}\in\mathbb{R}_+^2} -\mathbf{p_t}\mathbf{m_t^s} + V_t^s(\mathbf{m_t^s})}_{W_t^s(0,0)} \tag{C.3}$$

From (C.2)-(C.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.

In the second sub-period, with the chosen currency portfolios, a buyer and seller randomly enter the DM1, DM2, and DM3 with probabilities $\alpha_1, \alpha_2,$ and α_3, respectively. The problems faced by the buyer and seller in the second sub-period are exactly the same as in Section 4. More specifically, the DM value functions are described as (35)-(36); the solutions to the terms of trade in each decentralized market are given in Lemma 4.1; and the optimal currency portfolio of an agent satisfies Lemma 4.2.

C.2. Equilibrium

Definition C.1. *Given γ and ϵ, an equilibrium is a set of decision rules in the centralized market $\{x_t^b, \mathbf{m}_t^b, x_t^s, \mathbf{m}_t^s\}_{t=0}^{\infty}$, the terms of trade in each decentralized market $\{(q_t^1, d_t^{1,m}), (q_t^2, d_t^{2,c}), (q_t^3, d_t^{3,m}, d_t^{3,c})\}_{t=0}^{\infty}$, 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 (C.2)-(C.3) and (35)-(36); $\{(q_t^1, d_t^{1,m}), (q_t^2, d_t^{2,c}), (q_t^3, d_t^{3,m}, d_t^{3,c})\}$ solve problems (40)-(42); as well as market clearing for centralized good, fiat money, and cryptocurrency, and cryptocurrency law of motion 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 $M_{t+1}^c = (1+\epsilon-\pi)M_t^c$ where $1+\epsilon-\pi > \beta(1-\pi)$, according to (52)-(53), the equilibrium conditions satisfy:

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

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

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

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

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

C.3. Coexistence

Proposition C.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 $\beta(1-\pi) < 1+\epsilon-\pi < 1+\bar{\mu}$. The equilibrium outcomes are characterized by:*

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

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

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

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

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

[Proof of Proposition C.1]

Proof. In stationary equilibrium, $p_t^k M_t^k = p_{t+1}^k M_{t+1}^k, k \in \{m,c\}$. Given $\beta < \gamma < \bar{\gamma}$ and $\beta(1-\pi) < 1+\epsilon-\pi < 1+\bar{\mu}$, from (C.4)-(C.5), the real balances of two currencies, z_m and z_c, satisfy (C.8)-(C.9). Following Lemma 4.1, the steady state consumption of the DM good in each decentralized market satisfies (C.10)-(C.12). Given the functional forms $u(\cdot), \omega(\cdot)$, and parameters of the model, a set of equilibrium outcomes can be jointly determined by (C.8)-(C.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.

□