On the Coexistence of Cryptocurrency and Fiat Money

Zhixiu Yu*

August 2022

Abstract

This paper uses a search-theoretic model to study conditions under which cryptocurrency is valued and under which it coexists with fiat money. In my model, a cryptocurrency economy is one in which private agents' decisions determine the stock of money and in which the marginal cost of producing money is increasing in the existing nominal stock. I show that the inflation rate of cryptocurrency must be zero in a stationary monetary equilibrium. This result is in sharp contrast to models with fiat money in which the stock of money is exogenously given. In fiat money economies, the inflation rate is determined by the rate of growth of the money stock. My result is also in sharp contrast with other types of private money economies, in which the inflation rate must necessarily be different from zero. In such private money economies, the cost of producing additional money does not depend on the existing nominal stock. Moreover, I show that cryptocurrency and fiat money can circulate at the same time and that the rates of return on these two assets may not be the same. Competition with cryptocurrency restricts the government's ability to over-issue fiat money and thereby might improve on pure fiat money equilibria without government commitment.

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. Declarations of interest: none. 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, Oksana Leukhina, Qingxiao Li, Fernando Martin, Christopher Phelan, Guillaume Rocheteau, Agustin Samano, Dan Su, Neil Wallace, Christopher Waller, Randall Wright, Ariel Zetlin-Jones, Lichen Zhang, and Yu Zhu for their helpful comments and suggestions, as well as participants from the Public Workshop at the University of Minnesota, the 2019 Midwest Economics Association at St. Louis, the 2019 Summer Workshop on Money, Banking, Payment and Finance at the Bank of Canada, and the Macro Brownbag Seminar at the University of California Irvine.

1. Introduction

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

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

To that end, I first develop a search-theoretic model of an economy with a privately-produced money—cryptocurrency. My framework builds on the workhorse model of monetary exchange by Lagos and Wright (2005) and adds a new type of private agents—profit-maximizing miners—who are the sole issuers of cryptocurrency. The Lagos-Wright (LW) framework is particularly insightful for addressing currency issues because the acceptability of a medium of exchange is determined endogenously in equilibrium, and it is amenable to analysis and allows me to incorporate a miner sector while keeping the distribution of currency holdings analytically tractable.[1]

My model highlights two key attributes of cryptocurrency: it is private money, and it is costly to produce. Its supply is endogenous and driven by the production decisions of miners, who have access to a costly mining technology that recognizes the legitimacy of cryptocurrency. The cost of producing additional cryptocurrency increases not only in the number of new units, but also in the aggregate nominal stock. This is a key feature that makes cryptocurrency different from other types of private money in the literature, e.g., bank notes, since the production cost of those private monies is independent of their existing nominal stock. These assumptions are intended to capture the deflationary property of cryptocurrency. For example, when producing Bitcoin, there are costs

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

associated with the production, such as computer power and electricity, and the new bitcoin mining rewards halve every 210,000 blocks.[2] Thus, the cost of mining the same amount of bitcoin gets more expensive as more bitcoin is minted.[3] In the real world, however, there are myriad cryptocurrencies with different supply rules. For example, similar to Bitcoin, Litecoin and Handshake have a maximum attainable supply through halving new coin rewards after reaching a certain supply level. There are also some cryptocurrencies with no maximum supplies, including Ethereum and Dogecoin. Furthermore, the supply of some other cryptocurrencies is hard to quantify, for instance, Terra, which is minted and burned to maintain a 1:1 value with the U.S. dollar.[4] My model applies to cryptocurrencies whose marginal production costs depend on their nominal stock of money—a property of mainstream cryptocurrencies in the real world, such as Bitcoin.[5] More broadly, my model is applicable to any intrinsically worthless object that can be privately produced via a costly technology and serve as a medium of exchange.[6]

Moreover, I model the cryptocurrency law of motion by assuming that the stock of cryptocurrency in each period is determined by both the newly produced units and the depreciation from the last period. The amount of new cryptocurrency is endogenously determined by miners' decisions, while the depreciation is modeled to capture the loss of cryptocurrency. In particular, I assume that a proportion of the cryptocurrency holdings from the last period will be lost in each period. These assumptions are intended to capture the idea that cryptocurrency is more vulnerable to being lost because people sent it to a wrong address, or lost or discarded their device, or forgot their password which has complicated strings, etc.[7] Unlike most types of the medium of exchange, such as cash or

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

[3]Conceptually, gold has this in common with Bitcoin given its limited amount, making the production costs of gold depend on its existing stock. However, there are several differences between gold and cryptocurrency in this paper: (1) Gold is not intrinsically worthless and has fundamental values in use; and (2) Gold can be reused after it is lost and, therefore, it has a much lower or nearly no loss/depreciation rate. As a result, the gold economy cannot have the analog of the non-monetary and non-stationary equilibria, which are driven by the zero fundamental value. Likewise, in the case of the gold economy, there is no monetary equilibrium with a stable price and constantly newly produced units, which is driven by the cost function and positive depreciation rate.

[4]Some types of cryptocurrency destroy or burn a section of its supply on purpose, e.g., Terra and Binance Coin, to reduce the total amount in circulation. See more on `https://www.investopedia.com/tech/cryptocurrency-burning-can-it-manage-inflation/`.

[5]As of June 2022, Bitcoin accounts for 47% of the cryptocurrency market capitalization, according to CoinMarketCap. See more on `https://coinmarketcap.com`.

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

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

commodity money like gold, which can be reused after getting lost, once a cryptocurrency is lost, it might be lost forever, and other people cannot reuse it.[8]

In the economy with cryptocurrency only, I show that given that the marginal production cost increases in the existing nominal stock of money, the inflation rate must be zero in a stationary monetary equilibrium. My result is in sharp contrast to models with fiat money in which the stock of money is exogenously given, e.g., Lagos and Wright (2003, 2005). In fiat money economies, the inflation rate is determined by the rate of growth of the money stock, and it can be different from zero as long as the stock of money changes over time. My result is also in sharp contrast with other types of private money economies, in which the inflation rate must necessarily be different from zero, e.g., Fernández-Villaverde and Sanches (2018). In their private money economy, the production cost is independent of the existing money stock, and there is no currency depreciation. Profit-maximizing producers always have an incentive to create an additional unit of money and, thus, a monetary equilibrium necessarily has inflation. Their result does not hold in my cryptocurrency economy. Intuitively, in order to have an inflationary equilibrium, the aggregate nominal stock of cryptocurrency must be increasing. In my model, however, the marginal production cost increases in the aggregate nominal stock of money. It follows that, if the money stock goes up, the marginal cost increases, thereby weakening miners' incentives to mine and contradicting the supposition. Therefore, the inflationary equilibrium cannot be sustained. Likewise, a deflationary equilibrium requires that the nominal stock of cryptocurrency declines. Such an equilibrium cannot arise because it is inconsistent with the rising production incentives on the part of the miners. Thus, the price and stock of cryptocurrency must remain constant in a stationary equilibrium, and all the newly produced units replace the depreciated currency each period.

Next, to explore the coexistence of cryptocurrency and fiat money, I extend my cryptocurrency-only model by adding government-issued fiat money and multiple decentralized markets into the economy. Fiat money differs from cryptocurrency in the issuers, supply rules, production costs, and probabilities that agents visit the markets where sellers accept that currency as a payment method. Fiat money is costless to produce, and is exogenously supplied according to a deterministic growth rule. Each period agents randomly enter one of the three decentralized markets: DM1, DM2, and DM3, which differ in the currencies that can be used for transactions. Specifically, agents can only trade with fiat money in DM1, e.g., transactions that accept cash only or involve the government authorities; agents can only trade with cryptocurrency in DM2, e.g., online Bitcoin stores or black markets where fiat money is not used; and agents can trade with both currencies in DM3, e.g., AT&T, PayPal, Microsoft, etc.[9] This market structure is analogous to that of the two-currency,

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

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

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 Lucas (1982), which constrain agents to use one type of currency in a particular trade.

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

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

Further, when there exists a market where both currencies can be accepted, the real values of cryptocurrency and fiat money are interdependent, and the substitution between two currencies put constraints on government monetary policy. Specifically, when one currency becomes more costly to hold or less useful in decentralized markets, agents would demand less for that currency and instead substitute the other currency for transactions. As a result, the real value of that currency decreases, whereas the real value of the other one increases. In particular, cryptocurrency becomes more costly to carry if it is lost at a higher rate or its marginal production cost diminishes, whereas

[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.

fiat money becomes more costly to use if it is issued at a higher growth rate. A currency becomes more useful when its acceptability degree gets larger. Even under the case that cryptocurrency, in some sense, inferior in production costs and degrees of acceptability in decentralized markets, it can coexist with fiat money, an asset that is more acceptable and costless to produce, when appropriate monetary policy is implemented. As the inflation rate of cryptocurrency is zero in a stationary monetary equilibrium, the competition with cryptocurrency restricts the government's ability to over-issue fiat money for raising its seigniorage.

To further support the point where the monetary policy is constrained when fiat money competes with a private currency that is costly to produce, my model generates the Laffer curve and captures its changes with the introduction of cryptocurrency. The Laffer curve shows that the steady-state seigniorage first rises and then falls with increasing inflation because the higher inflation lowers the purchasing power of fiat money and thus discourages agents from holding it. As a result, there exists a fiat money growth rate that maximizes seigniorage earnings. In my two-currency economy, agents have a probability of entering the market where cryptocurrency is accepted alongside with fiat money. Compared to the fiat money economy, the Laffer curve with the introduction of cryptocurrency shrinks, and the government's seigniorage decreases. In particular, the peak of the Laffer curve shifts down and to the left, and the seigniorage-maximizing level of the money growth rate falls. The larger the market size in which both currencies can be accepted, the lower the seigniorage-maximizing money growth rate and the fewer seigniorage earnings when inflation rises.

The way that cryptocurrency can affect the circulation of fiat currency raises a question: should the government ban cryptocurrency? In the real world, there are many countries with different attitudes toward cryptocurrency and its regulations. While a number of countries like China have banned crypto mining, most countries like the United States and Canada hold a more neutral attitude towards cryptocurrency.[11] There also have been some countries, such as The Bahamas and Nigeria, that decided to create their own central bank-controlled digital currencies to compete with cryptocurrency.[12] Since the mining process of cryptocurrency requires large amounts of energy, it leads to concerns about energy waste and its negative impact on the environment.[13] On the other side, currency competition can be helpful in calming inflation and preventing the manipulation of interest rates and prices by the government.[14] My model suggests that whether or not the introduc-

[11]Here is a list of countries where Bitcoin is banned or legal: https://cryptonews.com/guides/countries-in-which-bitcoin-is-banned-or-legal.htm.

[12]See https://fortune.com/2022/01/13/9-countries-central-digital-currencies-crypto/.

[13]For example, members of the European Union Parliament recently proposed to ban the use of energy-intensive cryptocurrencies. See more on https://www.coindesk.com/policy/2022/02/24/eu-parliamentarians-push-to-limit-bitcoin-use-over-energy-concerns/. For more information on energy issues, see https://www.nytimes.com/2022/03/22/technology/bitcoin-miners-environment-crypto.html.

[14]For more information on discussions about whether or not cryptocurrencies interact with inflation and monetary policy, refer to https://voxeu.org/article/monetary-policy-world-cryptocurrencies and see

tion of cryptocurrency would improve welfare depends on the acceptability of cryptocurrency and the government's ability to commit to maintaining the targeted fiat money growth rule. Banning cryptocurrency can clearly save the resources used in its production, but it may worsen the total welfare of the economy. One reason for this is that, in the absence of cryptocurrency, agents would only trade using fiat money in decentralized markets, thereby missing out on the trade surplus in the market where only cryptocurrency is accepted. In that case, if the government tends to overissue fiat money, there would be additional welfare loss from consuming less output. However, if cryptocurrency is not widely accepted and the government can maintain sufficiently low inflation, then banning cryptocurrency would be welfare-enhancing. There would be welfare gains from avoiding resource waste associated with producing cryptocurrency and from consuming more output, which would outweigh the welfare loss from no trade surplus in the market where only cryptocurrency is used. As cryptocurrency is consistent with zero inflation in a stationary equilibrium, the government that tends to use the inflation tax would have a strong incentive to ban cryptocurrency.

My paper is related to two branches of a large literature on multiple currencies that are competing as media of exchange. One branch is the literature where no currency is privately produced, e.g., Kareken and Wallace (1981). The other branch, where my paper belongs, is the literature where at least one of those currencies is privately produced, e.g., Lagos and Rocheteau (2008). Different from these currency competition models in which two assets can coexist only if they have the same rate of return, my model shows that fiat money and cryptocurrency can coexist and that the rates of return on these two assets may not be the same. This is driven by the payment acceptability constraints in decentralized markets. Thus, each currency is essential in some transactions.[15]

There is a growing literature on cryptocurrency issues. For instance, Schilling and Uhlig (2019) analyze the price dynamics of Bitcoin. They show that bitcoin prices form a martingale, and the risk-adjusted real return on Bitcoin and the dollar has to be identical when both currencies are simultaneously in use. You and Rogoff (2019) study the competition between online retailer-issued tokens and bank debit accounts, and focus on issuers' sale and issuance strategies. My emphasis is different from theirs. I focus on the coexistence of cryptocurrency and fiat money in a stationary equilibrium, and I show that the two currencies can coexist with different rates of return. In addition, my paper has it in common with Choi and Rocheteau (2020b) and Zhu and Hendry (2019) that two competing currencies have different degrees of acceptability in decentralized meetings. However, one of the central points of my paper is to answer the question: If cryptocurrency is costly to produce and the aggregate new cryptocurrency is endogenously determined by miners' decisions, what sorts of equilibria are possible? In contrast, the aggregate mining rate of cryptocurrency is exogenously determined in Choi and Rocheteau (2020b), and the private money is costless to

`https://freopp.org/how-bitcoin-protects-americans-from-inflation-407522ebe391`.

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

produce in Zhu and Hendry (2019). Therefore, these papers cannot have an analog of the monetary equilibrium in which the price of cryptocurrency must be constant.

My paper is also related to an extensive literature on currency competition where the issuers of private money are costly operating sectors, e.g., banks. He et al. (2008) and Chari and Phelan (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 deposits are in safekeeping, but the bank is costly to operate. They show that with exogenous theft, there is no concurrent circulation of both currencies. In the latter paper, bank deposits serve a socially useful insurance role and are privately useful because the bank pays interest on deposits, but banks are costly and subject to bank runs. The authors show that there is no equilibrium in which fiat money and bank deposits coexist. My results are different from theirs. Cryptocurrency can coexist with fiat money in equilibrium, even if it is costly to produce. Moreover, unlike those papers with fractional reserve banking, there is no reserve requirement in my model, and the cryptocurrency that is produced by miners is not associated with any promise to exchange for goods or assets in the future.

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

2. A Model of Cryptocurrency Only

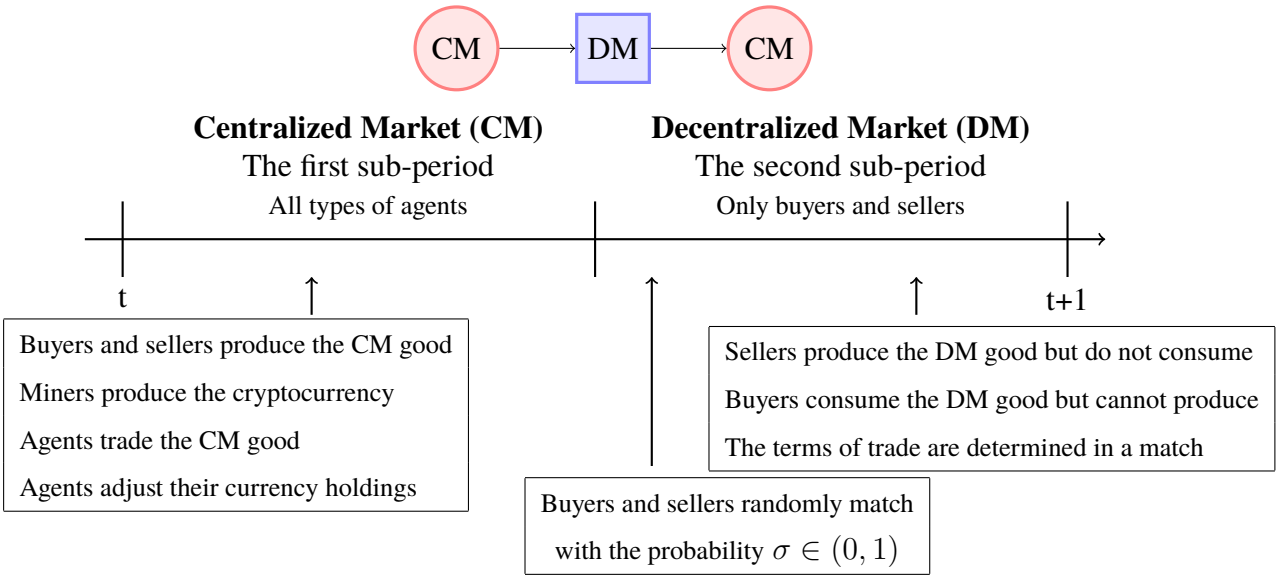
There are three types of infinitely lived agents in the economy: *buyers, sellers*, and *miners*. Each of them are populated with a [0,1]-continuum, and agents' types are permanent. Time is discrete and continues forever. Agents discount the future between periods with a discount factor $\beta \in (0,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

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

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

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



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

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

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

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

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

2.1. ***Cryptocurrency***

A medium of exchange is supplied only in the form of cryptocurrency. Its supply is endogenous and driven by the production decisions of profit-maximizing miners. Let M_t denote the aggregate nominal stock of cryptocurrency in period t. Each period, a typical miner i produces δ_t^i units of new cryptocurrency with the cost $c(\delta_t^i, M_{t-1})$, which satisfies the following assumption.

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

The cost of producing additional cryptocurrency increases not only in the number of new units, but also in the aggregate nominal stock. This assumption is intended to capture some important properties of cryptocurrency production costs in the real world. In the case of Bitcoin, for example, the mining process is exceptionally energy-intensive. Miners get new coin rewards through solving complicated computational problems using computers and servers that are programmed specifically for this purpose, with costs rising with computing power and electricity use. The difficulty level of those computational problems rises with the increased production, and the new coin rewards get cut in half when a certain amount of supply is reached, which causes the cost of producing additional units to increase in the aggregate supply.[17] This is a key feature of cryptocurrency that distinguishes it from fiat money and other types of private money, e.g., bank notes, since the production cost of those monies is independent of their existing stock.

[17] In reality, the production cost of Bitcoin is complicated to calculate. For instance, a miner's production cost also depends on the comparison of the computational power of the capital that the miner uses and that of all other miners. For more information on bitcoin production costs calculation, see `https://www.coinwarz.com/mining/bitcoin/calculator` and `https://medium.com/capriole/bitcoins-production-cost-88d889462ea7`.

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

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

The aggregate new cryptocurrency, Δ_t, is endogenously determined by miners' production decisions, and the currency depreciation, κM_{t-1}, captures the lost cryptocurrency, which cannot be reused by other people.[18] I assume that in each period, a proportion $\kappa \in (0, 1)$ of the cryptocurrency stock from the last period will be lost.[19]

Cryptocurrency is perfectly divisible, recognizable, and non-counterfeitable. It is also intrinsically worthless and is not associated with any promise to exchange for goods in the future.[20] An agent is able to predict miners' production behaviors by solving their maximization problems and form beliefs about the exchange value of cryptocurrency in current and future periods. Let $p_t \in \mathbb{R}_+$ denote the value of cryptocurrency per unit in terms of the CM good in period t.

2.2. *Buyers and sellers*

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

2.2.1. *The Centralized Market Problems*

In the first sub-period, a typical buyer b and seller s enter the centralized market with m^b_{t-1} and m^s_{t-1} units of cryptocurrency from the last period, respectively. In the market, a certain fraction, κ, of the cryptocurrency holdings that an agent brings to the market is lost. A typical buyer and seller choose their net consumption of the CM good, x^b_t and x^s_t, and cryptocurrency holdings, m^b_t and m^s_t, to bring forward to the decentralized market, respectively. The maximization problems of a buyer and seller in the centralized market are represented by:

$$W^j_t(m^j_{t-1}) = \max_{x^j_t, m^j_t} \quad x^j_t + V^j_t(m^j_t), \quad s.t. \quad x^j_t + p_t m^j_t = p_t(1-\kappa)m^j_{t-1}, \quad j \in \{b, s\} \tag{2}$$

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

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

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

where $W_t^j(m_{t-1}^j)$ denotes 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 $V_t^j(m_t^j)$ denotes 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, $j \in \{b, s\}$.

The above CM value functions can be rearranged as:

$$W_t^j(m_{t-1}^j) = p_t(1-\kappa)m_{t-1}^j + W_t^j(0), \quad j \in \{b, s\} \tag{3}$$

where $W_t^j(0) = \max_{m_t^j \in \mathbb{R}_+} -p_t m_t^j + V_t^j(m_t^j)$. Due to the idiosyncratic trading shocks in decentralized meetings, agents begin a period with different cryptocurrency holdings. Under the quasi-linear preferences, an agent's choice of cryptocurrency holdings in each period is independent of the initial cryptocurrency holdings when entering the centralized market and the cryptocurrency loss. Thus, the distribution of cryptocurrency holdings is degenerate to all agents of a given type at the beginning of each second sub-period.

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. A buyer randomly matches with a seller with the probability $\sigma \in (0, 1)$ and vice versa. In a match, the buyer makes a take-it-or-leave-it offer to the seller over the terms of trade, (q_t, d_t), which is given by the solution to:

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

The first constraint is the seller's participation constraint, and the second one is the buyer's liquidity constraint. If the seller accepts the offer, then the seller produces q_t units of the DM good with costs $\omega(q_t)$, whereas 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 and seller bring to the centralized market will be changed to $m_t^b - d_t$ and $m_t^s + d_t$, respectively.

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, $m_t^j, j \in \{b, s\}$.

The DM value functions of a typical buyer and seller are represented by:

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

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

2.2.3. *The Optimal Cryptocurrency Holdings*

Following Assumption 2.1 and (3), the optimal cryptocurrency holdings of a buyer and seller are given by the solutions to:

$$W_t^b(m_{t-1}^b) = \max_{m_t^b \in \mathbb{R}_+} -(p_t - p_{t+1}\beta(1-\kappa))m_t^b + v_t(m_t^b) \tag{7}$$

$$W_t^s(m_{t-1}^s) = \max_{m_t^s \in \mathbb{R}_+} -(p_t - p_{t+1}\beta(1-\kappa))m_t^s + 0 \tag{8}$$

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

Intuitively, in the centralized market, a buyer and seller choose cryptocurrency holding to maximize their expected surplus from using them in the decentralized market (the second terms on the right-hand side (RHS) of (7) and (8)) net of the costs of carrying them (the first terms on the RHS). Cryptocurrency is costly to carry when $\frac{p_t}{p_{t+1}} > \beta(1-\kappa)$. Since buyers make the take-it-or-leave-it offer in a match, they have all the bargaining power, and sellers have no surplus from trading in decentralized meetings.[21] Therefore, there is no strict incentive for sellers to carry cryptocurrency.

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

$$\frac{p_t}{\beta p_{t+1}(1-\kappa)} - 1 = \sigma[\frac{u' \circ \omega^{-1}(\beta p_{t+1}(1-\kappa)m_t^b)}{\omega' \circ \omega^{-1}(\beta p_{t+1}(1-\kappa)m_t^b)} - 1] \tag{9}$$

Different from previous LW literature with no currency depreciation, the cryptocurrency depreciation rate κ increases the cost of carry cryptocurrency and enters the money demand equation (9).[22]

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

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

[22] The optimal choices also satisfy the standard transversality condition $\lim_{t\to\infty} \beta^t p_t m_t = 0$; this will remain implicit in what follows. For a discussion about the necessity of transversality conditions in the optimization problems in infinitely-lived agent models, see, e.g., Rocheteau and Wright (2013).

production, $c(\delta_t^i, M_{t-1})$, which depend on the newly produced units and the existing nominal stock.[23] Since miners have no transaction demand in the decentralized market, they do not hold cryptocurrency, and they sell all newly produced units at price p_t right after production.[24] The maximization problem of a typical miner in period t is represented by:

$$\max_{x_t^i, \delta_t^i} \quad x_t^i, \quad s.t. \quad x_t^i \leq p_t \delta_t^i - c(\delta_t^i, M_{t-1}) \tag{10}$$

The above miner's problem can be written as follows.

$$\max_{\delta_t^i \geq 0} \quad p_t \delta_t^i - c(\delta_t^i, M_{t-1}) \tag{11}$$

Lemma 2.2. *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:*

$$\delta_t^i = c_\delta^{-1}(\max\{p_t, c_\delta(0, M_{t-1})\}) \tag{12}$$

where c_δ is the partial derivative of the cost function $c(\delta_t^i, M_{t-1})$ with respect to δ.

Example 2.1. *Suppose the production cost function of cryptocurrency is taken the functional form: $c(\delta_t, M_{t-1}) = DM_{t-1}\delta_t + B\delta_t^2,\ B, D > 0$, which satisfies Assumption 2.2. In this case, a miner i would produce $\delta_t^i = \max[0, \frac{p_t - DM_{t-1}}{2B}]$ units of cryptocurrency in period t.*[25]

From (12), the amount of new cryptocurrency in each period depends on the value and the aggregate stock of money. Further, the aggregate new cryptocurrency in period t, Δ_t, becomes:

$$\Delta_t = \int_0^1 \delta_t^i di = c_\delta^{-1}(\max\{p_t, c_\delta(0, M_{t-1})\}) \tag{13}$$

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

[23] The production cost of cryptocurrency is modeled as a resource cost in the paper. All the results would be the same if the production cost is modeled as a utility cost. Different from my model assumptions, Choi and Rocheteau (2020a) assume that miners produce private monies according to a time-consuming technology and face opportunity costs due to occupation choice.

[24] Appendix E.1 relaxes this assumption and shows that, even if miners are allowed to carry cryptocurrency, they would still choose to sell all the newly produced units after the production in equilibrium.

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

3. Equilibrium

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

1. $x_t^b, m_t^b, x_t^s, m_t^s$ *solve problems (2) and (5)-(6) for buyers and sellers;*
2. q_t, d_t *solve problem (4);*
3. x_t^i, δ_t^i *solve problem (10) for miners;*
4. *the cryptocurrency law of motion is satisfied:*
   $M_t = (1-\kappa)M_{t-1} + \Delta_t$*, where* Δ_t *satisfies (13);*
5. *the cryptocurrency market clear:*
   $M_t = M_t^b + M_t^s$*, where* $M_t^b = \int_0^1 m_t^b db,\ M_t^s = \int_0^1 m_t^s ds$*;*
6. *the centralized good market clear:*
   $\int_0^1 x_t^b db + \int_0^1 x_t^s ds + \int_0^1 x_t^i di + \int_0^1 c(\delta_t^i, M_{t-1}) di = 0$*.*

An equilibrium is a monetary equilibrium if the price of cryptocurrency is strictly greater than zero and a non-monetary equilibrium otherwise. A stationary equilibrium is an equilibrium in which the real balance of cryptocurrency is constant over time, i.e., $p_t M_t = p_{t+1} M_{t+1} = z^{ss}\ \ \forall t$*.*

I first characterize the stationary equilibrium in the cryptocurrency-only economy. Since cryptocurrency has no intrinsic value, there is always a non-monetary stationary equilibrium s.t. $p_t = p_{t+1} = 0$, and therefore, $z^{ss} = 0\ \forall t$. In what follows, I focus on the stationary equilibrium in which cryptocurrency is valued and produced.[26] I investigate the existence of the equilibrium in which the price changes at a constant rate or the price remains constant.

Proposition 1. *Under Assumptions 2.1 and 2.2, there is no stationary monetary equilibrium in which the price of cryptocurrency changes at a constant rate. There exists a unique stationary monetary equilibrium in which the price of cryptocurrency is constant. The equilibrium outcomes are characterized by:*

$$\frac{1-\beta(1-\kappa)}{\sigma\beta(1-\kappa)} = \left[\frac{u' \circ \omega^{-1}(\beta z^{ss}(1-\kappa))}{\omega' \circ \omega^{-1}(\beta z^{ss}(1-\kappa))} - 1\right] \tag{14}$$

$$c_\delta^{-1}(p^{ss}) = \kappa M^{ss} \tag{15}$$

$$1 + \frac{1-\beta(1-\kappa)}{\sigma\beta(1-\kappa)} = \frac{u'(q^{ss})}{\omega'(q^{ss})} \tag{16}$$

$$\Delta^{ss} = \kappa M^{ss} \tag{17}$$

[26] Appendix A.2 presents a stationary monetary equilibrium in an economy without cryptocurrency production.

Proposition 1 presents the main result of the cryptocurrency economy: Given that the marginal cost of producing cryptocurrency strictly increases in the aggregate stock of money, there exists a stationary equilibrium in which cryptocurrency is valued, and the inflation rate must be zero in equilibrium. That is, the price and stock of cryptocurrency remain constant, which are jointly determined by (14) and (15), and all the newly produced units only replace the depreciated currency in each period, i.e., $\Delta^{ss} = \kappa M^{ss}$. It is necessary to have currency loss/depreciation in order for a stationary monetary equilibrium with constantly produced new money to exist. If there is no currency loss, then no new cryptocurrency is produced in equilibrium. Moreover, as Proposition 1 shows, the equilibrium quantity traded in the decentralized market is less than the socially efficient quantity, $q^{ss} < q^*$. The stationary monetary equilibrium with a stable price of cryptocurrency is not socially efficient.

Why must the price of cryptocurrency be constant in a stationary monetary equilibrium? Intuitively, in order to have an inflationary equilibrium, the aggregate nominal stock of cryptocurrency must be increasing. However, in my model, the cost of producing additional cryptocurrency increases in the aggregate nominal stock of money. It follows that, if the stock of money goes up, the real marginal production cost increases, thereby weakening miners' production incentives and contradicting the supposition. Therefore, the inflationary equilibrium cannot be sustained. Likewise, a deflationary equilibrium requires that the nominal stock of cryptocurrency declines. Such an equilibrium cannot arise because it is inconsistent with the rising production incentives of miners due to the high return on money. Therefore, the price and nominal stock of cryptocurrency have to be stable in equilibrium. My analysis confirms the conjecture in Hayek (1999) that a purely private arrangement would deliver price stability.

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

Further, my result is also in sharp contrast to other types of private money economies, in which the inflation rate must necessarily be different from zero. For example, Fernández-Villaverde and Sanches (2018) show that a monetary equilibrium with private monies that are issued by profit-maximizing entrepreneurs, in general, will not deliver price stability. In their private money economy, the cost of production additional money is independent of the existing nominal stock, e.g., the marginal cost goes to zero as newly produced money goes to zero, and there is no currency depreciation. In that case, entrepreneurs always have an incentive to create an additional unit of

private money, which would make the money stock keep increasing under price stability. However, in the context of cryptocurrency, because the marginal production cost strictly increases in the nominal stock of money, which is subject to currency depreciation, miners do not have an incentive to produce cryptocurrency in excess of the flow of currency exogenously lost. Therefore, the price of cryptocurrency remains constant in equilibrium. The result of Fernández-Villaverde and Sanches (2018) does not hold in the private money environment with the cost function satisfying Assumption 2.2.

If I make the marginal production cost of private money independent of the aggregate nominal stock in my model and set the currency depreciation rate to zero, as in the Fernández-Villaverde and Sanches economy, a monetary equilibrium would necessarily have positive inflation.[27] Intuitively, in order to have an equilibrium with a stable price, the aggregate nominal stock of money must be constant. However, given the new shape of the cost function, miners always have an incentive to produce additional new units of private money when the money is valued. Therefore, the aggregate money stock cannot remain constant given zero currency depreciation. Thus, the equilibrium consistent with price stability cannot be sustained. Further, we cannot have a deflationary equilibrium either because miners would produce more new units due to the high return on money. Therefore, the nominal stock of money cannot be decreasing in equilibrium. Thus, the result of Fernández-Villaverde and Sanches is correct in a version of my model with different assumptions about technology.[28]

In addition to stationary equilibria, in the cryptocurrency economy, there also exists a continuum of non-stationary equilibria in which the values of cryptocurrency converge to zero.[29] Cryptocurrency is intrinsically worthless and is traded due to its liquidity services in decentralized meetings. Agents in the economy form their beliefs about the values of cryptocurrency in future periods. For an initial cryptocurrency value less than its steady-state value, there exists an equilibrium path that the currency values depreciate and converge to zero. Along the inflationary equilibrium trajectory, the expected depreciating currency values lead the real balances of cryptocurrency to decline and converge to zero. In this situation, agents' beliefs about the depreciating value of cryptocurrency can be self-fulfilling. This result is similar to what happens in models with government-issued fiat money, e.g., Lagos and Wright (2003), and in models with other types of private money, e.g., Fernández-Villaverde and Sanches (2019). Cryptocurrency is subject to a self-fulfilling prophecy, even under the existence of a monetary equilibrium with a stable price.

[27] For example, the cost function, $c(\delta_t^i)$, is increasing, convex and twice differentiable, and satisfies $c'(0) = 0$.

[28] If private money has a positive depreciation rate, there is no inflationary equilibrium. Even though the marginal cost is independent of the nominal stock of money, decreasing currency values weaken miners' incentives to produce money in excess of depreciated currency. Therefore, the aggregate money stock cannot be increasing. Refer to Appendix C for a formal discussion about the equilibria of the private money economy with the alternative cost function.

[29] See Appendix A.3 for details about the non-stationary equilibria of the cryptocurrency economy.

4. Two-Currency Model

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

4.1. Currencies

Let cryptocurrency be indexed by c and fiat money be indexed by m. Cryptocurrency is modeled in the same way as in Section 2. 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.[30] In this paper, I treat γ as an exogenous variable. Let p_t^m denote the value of fiat money per unit in terms of the CM good in period t. Accordingly, the lump-sum transfers/taxes from the government in period t, expressed in terms of the CM good, are $T_t = p_t^m(\gamma - 1)M_{t-1}^m$.

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

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

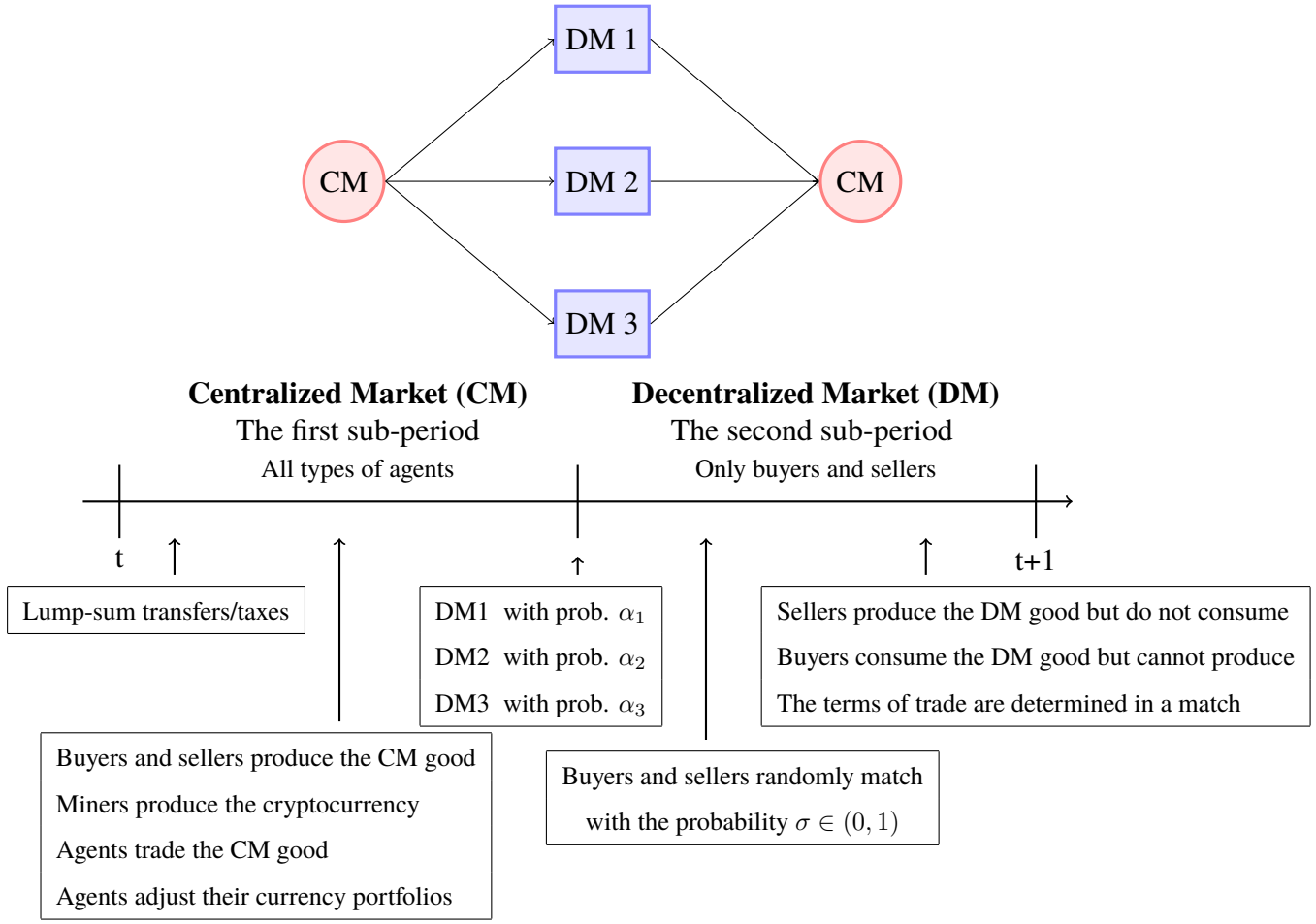
[30] The government can only tax agents in the centralized market because agents are anonymous and cannot be monitored in the decentralized market. Alternatively, Andolfatto (2013) considers lump-sum tax obligations as a form of debt subject to default. In that case, agents who fail to pay taxes in the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

4.2. *Environment*

The monetary environment is similar to that in Section 2. There are three types of infinitely lived agents: *buyers, sellers,* and *miners*, and each time period is divided into two sub-periods.[31]

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.

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



[31]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).

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. In particular, a buyer is randomly matched with a seller with $\sigma \in (0,1)$ and vice versa. In each match, the terms of trade are determined by a take-it-or-leave-it offer by the buyer. If 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. The utility and cost functions of the DM good are specified in Assumption 2.1.

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

4.3. Miners

Miners are only active during the first sub-period. In the centralized market, a typical miner i chooses the consumption of the CM good, x_t^i, produces δ_t^i units of cryptocurrency, and sells all the newly produced units at the price p_t^c right after production. Since miners remain idle in the second sub-period, they do not have transaction demand for the two currencies in decentralized markets. Without loss of generality, I assume that miners do not carry fiat money.[32]

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

$$\max_{x_t^i, \delta_t^i \geq 0} x_t^i \quad s.t. \quad x_t^i \leq p_t^c \delta_t^i - c(\delta_t^i, M_{t-1}^c) \tag{18}$$

where the production cost function satisfies Assumption 2.2.

Similar to the cryptocurrency-only economy, a miner i's production decision in period t depends on the value and nominal stock of cryptocurrency, such that

$$\delta_t^i = c_\delta^{-1}(\max\{p_t^c, c_\delta(0, M_{t-1}^c)\}) \tag{19}$$

The aggregate new cryptocurrency in period t, Δ_t, is the same as (13) with $p_t = p_t^c$ and $M_t = M_t^c$.

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

4.4. *Buyers and Sellers*

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

4.4.1. *The Centralized Market Problems*

A typical buyer b and seller s begin a period with their currency portfolios from the last period, $\mathbf{m}_{t-1}^{j} = (m_{t-1}^{m,j}, m_{t-1}^{c,j})$, which comprise $m_{t-1}^{m,j}$ units of fiat money and $m_{t-1}^{c,j}$ units of cryptocurrency, $j \in \{b, s\}$. Due to different trading histories in decentralized meetings, agents begin a period with different currency portfolios. In the market, a certain fraction κ of the cryptocurrency holdings is lost, and buyers receive lump-sum transfers/taxes T_t from the government. In the first sub-period, buyers and sellers 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, $\mathbf{m}_{t-1}^j \in \mathbb{R}_+^2$, and $V_t^j(\mathbf{m}_t^j)$ denote the value function of an agent beginning the second sub-period with the chosen currency portfolio, $\mathbf{m}_t^j \in \mathbb{R}_+^2$, $j \in \{b, s\}$. The CM maximization problems of a typical buyer and seller are represented by:

$$W_t^b(\mathbf{m_{t-1}^b}) = \max_{x_t^b, \mathbf{m_t^b}} \; x_t^b + V_t^b(\mathbf{m_t^b}) \quad s.t. \quad x_t^b + \mathbf{p_t m_t^b} = p_t^m m_{t-1}^{m,b} + (1-\kappa) p_t^c m_{t-1}^{c,b} + T_t \tag{20}$$

$$W_t^s(\mathbf{m_{t-1}^s}) = \max_{x_t^s, \mathbf{m_t^s}} \; x_t^s + V_t^s(\mathbf{m_t^s}) \quad s.t. \quad x_t^s + \mathbf{p_t m_t^s} = p_t^m m_{t-1}^{m,s} + (1-\kappa) p_t^c m_{t-1}^{c,s} \tag{21}$$

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 (20)-(21) can be rearranged as:

$$W_t^j(\mathbf{m_{t-1}^j}) = p_t^m m_{t-1}^{m,j} + (1-\kappa) p_t^c m_{t-1}^{c,j} + W_t^j(0,0) \tag{22}$$

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

4.4.2. *The Decentralized Markets Problems*

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

$$
\begin{aligned}
V_t^b(\mathbf{m_t^b}) = & \max_{(q_t^1,d_t^{1,m}),(q_t^2,d_t^{2,c}),(q_t^3,d_t^{3,m},d_t^{3,c})} \alpha_1\{\sigma[u(q_t^1)+\beta W_{t+1}^b(m_t^{m,b}-d_t^{1,m},m_t^{c,b})]+(1-\sigma)\beta W_{t+1}^b(\mathbf{m}_t^b)\} \\
& +\alpha_2\{\sigma[u(q_t^2)+\beta W_{t+1}^b(m_t^{m,b},m_t^{c,b}-d_t^{2,c})]+(1-\sigma)\beta W_{t+1}^b(\mathbf{m}_t^b)\} \\
& +\alpha_3\{\sigma[u(q_t^3)+\beta W_{t+1}^b(m_t^{m,b}-d_t^{3,m},m_t^{c,b}-d_t^{3,c})]+(1-\sigma)\beta W_{t+1}^b(\mathbf{m_t^b})\}
\end{aligned} \tag{23}
$$

$$
\begin{aligned}
V_t^s(\mathbf{m_t^s}) = & \alpha_1\{\sigma[-\omega(q_t^1)+\beta W_{t+1}^s(m_t^{m,s}+d_t^{1,m},m_t^{c,s})]+(1-\sigma)\beta W_{t+1}^s(\mathbf{m}_t^s)\} \\
& +\alpha_2\{\sigma[-\omega(q_t^2)+\beta W_{t+1}^s(m_t^{m,s},m_t^{c,s}+d_t^{2,c})]+(1-\sigma)\beta W_{t+1}^s(\mathbf{m}_t^s)\} \\
& +\alpha_3\{\sigma[-\omega(q_t^3)+\beta W_{t+1}^s(m_t^{m,s}+d_t^{3,m},m_t^{c,s}+d_t^{3,c})]+(1-\sigma)\beta W_{t+1}^s(\mathbf{m_t^s})\}
\end{aligned} \tag{24}
$$

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

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

$$
\begin{aligned}
\text{In DM1:} \quad & \max_{q_t^1,d_t^1} \quad u(q_t^1)+\beta W_{t+1}^b(m_t^{m,b}-d_t^{1,m},m_t^{c,b}) \\
s.t. \quad & -\omega(q_t^1)+\beta W_{t+1}^s(m_t^{m,s}+d_t^{1,m},m_t^{c,s}) \geq \beta W_{t+1}^s(m_t^{m,s},m_t^{c,s}) \\
& d_t^{1,m} \leq m_t^{m,b}
\end{aligned} \tag{25}
$$

$$
\begin{aligned}
\text{In DM2:} \quad & \max_{q_t^2,d_t^2} \quad u(q_t^2)+\beta W_{t+1}^b(m_t^{m,b},m_t^{c,b}-d_t^{2,c}) \\
s.t. \quad & -\omega(q_t^2)+\beta W_{t+1}^s(m_t^{m,s},m_t^{c,s}+d_t^{2,c}) \geq \beta W_{t+1}^s(m_t^{m,s},m_t^{c,s}) \\
& d_t^{2,c} \leq m_t^{c,b}
\end{aligned} \tag{26}
$$

$$
\begin{aligned}
\text{In DM3:} \quad & \max_{q_t^3,d_t^{3,m},d_t^{3,c}} \quad u(q_t^3)+\beta W_{t+1}^b(m_t^{m,b}-d_t^{3,m},m_t^{c,b}-d_t^{3,c}) \\
s.t. \quad & -\omega(q_t^3)+\beta W_{t+1}^s(m_t^{m,s}+d_t^{3,m},m_t^{c,s}+d_t^{3,c}) \geq \beta W_{t+1}^s(m_t^{m,s},m_t^{c,s}) \\
& d_t^{3,m} \leq m_t^{m,b}, d_t^{3,c} \leq m_t^{c,b}
\end{aligned} \tag{27}
$$

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

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

Next, following Assumption 2.1 and (22), the optimal currency portfolios of a buyer and seller are given by the solutions to:

$$W_t^b(\mathbf{m}_{t-1}^b) = \max_{m_t^{m,b}, m_t^{c,b} \in \mathbb{R}_+^2} -(p_t^m - \beta p_{t+1}^m) m_t^{m,b} - (p_t^c - \beta(1-\kappa) p_{t+1}^c) m_t^{c,b} + v_t^{1,b}(m_t^{m,b}) + v_t^{2,b}(m_t^{c,b}) + v_t^{3,b}(\mathbf{m}_t^b) \tag{28}$$

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

$$W_t^s(\mathbf{m}_{t-1}^s) = \max_{m_t^{m,s}, m_t^{c,s} \in \mathbb{R}_+^2} -(p_t^m - \beta p_{t+1}^m) m_t^{m,s} - (p_t^c - \beta(1-\kappa) p_{t+1}^c) m_t^{c,s} + 0 + 0 + 0 \tag{29}$$

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. The first two terms on the RHS of (28)-(29) represent the cost of carrying fiat money and cryptocurrency to the next period, while the last three terms represent the expected surplus from trading in each decentralized market.

Cryptocurrency is costly to carry when $p_t^c > \beta p_{t+1}^c (1-\kappa)$, and fiat money is costly to carry when $p_t^m > \beta p_{t+1}^m$. Since buyers are the ones to make the offer, they take all the gains from trading. Sellers have no trade surplus in any decentralized market and, thus, there is no strict incentive for them to carry currency portfolios forward to the second sub-period.

5. Equilibrium

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

Definition 2. *Given γ, an equilibrium is a set of decision rules in the centralized market $\{x_t^b, \mathbf{m}_t^b, x_t^s, \mathbf{m}_t^s, x_t^i, \delta_t^i\}_{t=0}^{\infty}$, the terms of trade in each decentralized market $\{(q_t^1, d_t^{1,m}), (q_t^2, d_t^{2,c}), (q_t^3, d_t^{3,m}, d_t^{3,c})\}_{t=0}^{\infty}$, sequences of values of the two currencies $\{p_t^c, p_t^m\}_{t=0}^{\infty}$, and the aggregate stock of cryptocurrency $\{M_t^c\}_{t=0}^{\infty}$, such that for all $t \geq 0$: $\{x_t^b, \mathbf{m}_t^b, x_t^s, \mathbf{m}_t^s\}$ solve problems (20)-(21) and (23)-(24); $\{x_t^i, \delta_t^i\}$ solve problem (18); $\{(q_t^1, d_t^{1,m}), (q_t^2, d_t^{2,c}), (q_t^3, d_t^{3,m}, d_t^{3,c})\}$ solve problems (25)-(27); as well as market clearing for centralized good, fiat money, and cryptocurrency, and the cryptocurrency law of motion are satisfied.*

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

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

Suppose that, in general, the supplies of fiat money and cryptocurrency grow at constant rates, such that $M_{t+1}^m = \gamma M_t^m$ where $\gamma > \beta$ and $M_{t+1}^c = (1+\mu)M_t^c$ where $\mu > -\kappa$. Since sellers and miners have no incentive to carry currencies out of the centralized market, following Lemma A.5 and market clear conditions, the equilibrium conditions can be expressed as follows:

$$i_m \geq \alpha_1 \sigma L(\frac{z_m}{\gamma}) + \alpha_3 \sigma L(\frac{z_m}{\gamma} + \frac{(1-\kappa)z_c}{1+\mu}) \qquad \text{“}=\text{”} \text{ if } z_m > 0 \tag{30}$$

$$i_c \geq \alpha_2 \sigma L(\frac{(1-\kappa)z_c}{1+\mu}) + \alpha_3 \sigma L(\frac{z_m}{\gamma} + \frac{(1-\kappa)z_c}{1+\mu}) \qquad \text{“}=\text{”} \text{ if } z_c > 0 \tag{31}$$

where $i_m = \frac{p_t^m}{\beta p_{t+1}^m} - 1$ and $i_c = \frac{p_t^c}{\beta p_{t+1}^c (1-\kappa)} - 1$ denote the costs of carrying fiat money and cryptocurrency, respectively, which depend on the rate of return, time preference, and the currency depreciation rate.[33] According to (30)-(31), a currency is not valued when the cost of carrying it outweighs the expected payoff of using it in decentralized markets. The government can affect an agent's incentive to make currency portfolio choices through changing the monetary policy on the growth rule of the fiat money supply.

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

A non-monetary stationary equilibrium, in which no currency is valued, occurs when both

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

currencies are too costly to hold, i.e., $i_m \geq \alpha_1\sigma L(0) + \alpha_3\sigma L(0)$ and $i_c \geq \alpha_2\sigma L(0) + \alpha_3\sigma L(0)$. Accordingly, given the parameters and functional forms of the model, a unique non-monetary stationary equilibrium, $z_m = z_c = 0$, exists, so long as $\gamma \geq \tilde{\gamma}$ and $(1+\mu) \geq 1+\tilde{\mu}$, where $\tilde{\gamma}$ and $\tilde{\mu}$ are given by:

$$\frac{\tilde{\gamma}}{\beta} - 1 = \alpha_1\sigma L(0) + \alpha_3\sigma L(0) \tag{32}$$

$$\frac{1+\tilde{\mu}}{\beta(1-\kappa)} - 1 = \alpha_2\sigma L(0) + \alpha_3\sigma L(0) \tag{33}$$

A stationary equilibrium in which only fiat money is valued occurs when cryptocurrency is too costly to hold while fiat money is not. That is, $i_m = \alpha_1\sigma L(z_m/\gamma) + \alpha_3\sigma L(z_m/\gamma)$ and $i_c \geq \alpha_2\sigma L(0) + \alpha_3\sigma L(z_m/\gamma)$. This might happen when the size of the markets where sellers accept cryptocurrency for transactions is too small, or when the cryptocurrency depreciation rate is large, or when the rate of return on cryptocurrency is sufficiently low. Thus, a stationary equilibrium in which $z_m > 0$ and $z_c = 0$ exists, so long as $\beta < \gamma < \tilde{\gamma}$ and $1+\mu \geq 1+\bar{\mu}$, where $\tilde{\gamma}$ is from (32) and $\bar{\mu}$ is given by:

$$\frac{1+\bar{\mu}}{\beta(1-\kappa)} - 1 = \alpha_2\sigma L(0) + \frac{\alpha_3}{\alpha_1+\alpha_3}\left(\frac{\gamma}{\beta} - 1\right) \tag{34}$$

Symmetrically, a stationary equilibrium in which only cryptocurrency is valued, i.e., $z_m = 0$ and $z_c > 0$, exists so long as $\gamma \geq \bar{\gamma}$ and $1-\kappa < 1+\mu < 1+\tilde{\mu}$, where $1+\tilde{\mu}$ is from (33) and $\bar{\gamma}$ is given by:

$$\frac{\bar{\gamma}}{\beta} - 1 = \alpha_1\sigma L(0) + \frac{\alpha_3}{\alpha_2+\alpha_3}\left(\frac{1+\mu}{\beta(1-\kappa)} - 1\right) \tag{35}$$

Lastly, a stationary equilibrium in which both currencies are valued, i.e., $z_m > 0$ and $z_c > 0$, exists so long as $\beta < \gamma < \bar{\gamma}$ and $1-\kappa < 1+\mu < 1+\bar{\mu}$, where $\bar{\gamma}$ and $\bar{\mu}$ are given by (35) and (34), respectively.

5.1. Coexistence

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

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

$$\frac{\gamma-\beta}{\sigma\beta}=\alpha_1[\frac{u'\circ\omega^{-1}(\beta\frac{z_m}{\gamma})}{\omega'\circ\omega^{-1}(\beta\frac{z_m}{\gamma})}-1]+\alpha_3[\frac{u'\circ\omega^{-1}(\beta(\frac{z_m}{\gamma}+z_c(1-\kappa)))}{\omega'\circ\omega^{-1}(\beta(\frac{z_m}{\gamma}+z_c(1-\kappa)))}-1] \tag{36}$$

$$\frac{1-\beta(1-\kappa)}{\sigma\beta(1-\kappa)}=\alpha_2[\frac{u'\circ\omega^{-1}(\beta z_c(1-\kappa))}{\omega'\circ\omega^{-1}(\beta z_c(1-\kappa))}-1]+\alpha_3[\frac{u'\circ\omega^{-1}(\beta(\frac{z_m}{\gamma}+z_c(1-\kappa)))}{\omega'\circ\omega^{-1}(\beta(\frac{z_m}{\gamma}+z_c(1-\kappa)))}-1] \tag{37}$$

$$c_\delta^{-1}(p_c^{ss})=\kappa M_c^{ss} \tag{38}$$

$$q_1^{ss}=\omega^{-1}(\beta\frac{z_m}{\gamma}) \tag{39}$$

$$q_2^{ss}=\omega^{-1}(\beta z_c(1-\kappa)) \tag{40}$$

$$q_3^{ss}=\omega^{-1}(\beta\frac{z_m}{\gamma}+\beta z_c(1-\kappa)) \tag{41}$$

$$\Delta^{ss}=\kappa M_c^{ss} \tag{42}$$

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 (36)-(42) so long as $\beta<\gamma<\bar{\gamma}$ and $0<\hat{\mu}$, where $\bar{\gamma}$ is obtained from (35) with $\mu=0$, and $\hat{\mu}$ is given by (34) with $\gamma=\beta$.

Cryptocurrency and fiat money can coexist in equilibrium regardless of their rates of return. This is driven by the assumption that the two currencies have different degrees of acceptability in decentralized markets (e.g., Zhu and Hendry (2019)). Since each currency is essential in some meetings, agents will hold both currencies to smooth their consumption in all decentralized meetings, even if one has a higher inflation rate.

Moreover, my two-currency model has a novelty compared to other models of multiple competing currencies with payment acceptability constraints, such as a model of fiat monies, e.g., Zhang (2014), and a model of private and fiat monies, e.g., Zhu and Hendry (2019). In their models, the cost of carrying one currency is tied with the exogenous growth rate of the money supply. However, in my model, the cost of carrying cryptocurrency depends not only on the exogenous parameters, such as currency depreciation, but also on the endogenous production decisions of miners, which rely on the production cost function and further affect the price path of cryptocurrency in equilibrium. That is because the supply of cryptocurrency is endogenously determined by miners' decisions, and the shape of the cost function determines the relationship between equilibrium prices, aggregate money stock, and miners' production incentives through their profit maximization problems. Given that the marginal cost of producing money strictly increases in the existing nominal stock, the price and stock of cryptocurrency must remain constant in the equilibrium with both currencies in circulation.[34] In the next section, I explore how the model fundamentals affect the two currencies.

[34] Appendix D presents a two-currency economy where both cryptocurrency and fiat money are exogenously supplied. It shows that an economy with exogenously supplied cryptocurrency cannot have an analog of the equilibrium in which the price of cryptocurrency must remain constant.

5.1.1. Comparative Statics

Following Proposition 2, the real value of fiat money is interdependent with that of cryptocurrency when $\alpha_3 \neq 0$. In this case, the government's monetary policy can affect the values of currencies, and thus, the quantity of DM good traded with each currency. Intuitively, buyers can make offers on any arbitrary mix of the two currencies in DM3. As the fiat money inflates (i.e., γ increases), it becomes more costly to use fiat money. Agents would demand less for it and instead substitute into cryptocurrency, which decreases the real value of fiat money and increases that of cryptocurrency. As a monetary equilibrium with coexistence is consistent with a zero inflation rate in cryptocurrency, the competition with cryptocurrency restricts the government's ability to over-issue fiat money to raise the inflation tax.

In addition, if cryptocurrency is lost at a higher rate (i.e., κ increases), or if its marginal production cost diminishes (i.e., $c_\delta(\delta, M^c)$ decreases), the cost of carrying cryptocurrency increases.[35] Accordingly, agents would demand less for cryptocurrency and demand more for fiat money in decentralized meetings, which decreases the real value of cryptocurrency and increases that of fiat money. Moreover, as κ increases, the region of parameter $\bar{\gamma}$ increases. In this case, both currencies would still be valued in equilibrium when the government issues fiat money at a higher rate, as long as the new growth rate is less than the new parameter region $\bar{\gamma}$.

Further, if the acceptability degree of one currency gets larger, that currency becomes more useful in decentralized markets and thus has a higher expected payoff from using it. Then agents would demand more for that currency and the real value of it would increase. The following section explores the coexistence of the two currencies under special cases in terms of the market size. Table 1 summarizes the effects of the cost of carrying each currency and the market size on the real values of the two currencies. Calculations are provided in Appendix G.

5.1.2. Special Cases

The market size $\alpha_3 \neq 0$ is necessary for substitution between two currencies to put constraints on government monetary policy. When $\alpha_3 = 0$, there are two completely segmented decentralized markets in the economy. Since each currency is essential in some transactions, cryptocurrency and fiat money can coexist in a stationary equilibrium, but there is a dichotomy between the two curren-

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

Table 1: Comparative Statics

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

cies' sectors. Specifically, the real values of cryptocurrency and fiat money are independent, and the quantity of the DM good traded with cryptocurrency in DM2 is determined independently from that traded with fiat money in DM1. Government monetary policy, γ, has no effects on the value and demand for cryptocurrency use. The equilibrium outcomes only depend on the fundamentals of the economy, such as preferences, technologies, and trading frictions.[36]

In another case, when $\alpha_3 \neq 0$ and $\alpha_1 = 0$, cryptocurrency has an inherent advantage relative to fiat money because it is accepted everywhere, whereas fiat money is only accepted in DM3. In this set-up, agents would carry cryptocurrency to facilitate all kinds of transactions in decentralized markets. 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, i.e., $\gamma < \bar{\gamma} \equiv \alpha_3(\frac{1}{1-\kappa} - \beta) + \beta$, in the equilibrium with both currencies in circulation. Therefore, there exists a stationary equilibrium in which both currencies are valued, as long as fiat money is issued at a growth rate below a certain level $\bar{\gamma}$. Further, fiat money has to be issued at an even lower growth rate than $\bar{\gamma}$ when it becomes less acceptable (e.g., $\alpha_3 \downarrow$), or when cryptocurrency is less costly to carry (e.g., $\kappa \downarrow$), in order to be valued in the economy. Otherwise, only cryptocurrency is valued and circulating in the economy.

Symmetrically, when $\alpha_3 \neq 0$ and $\alpha_2 = 0$, there is an inherent advantage to fiat money. Agents will carry fiat money to facilitate all kinds of transactions in decentralized meetings. They will also carry cryptocurrency when the rate of return on it is sufficiently higher than that on fiat money. That is, fiat money is issued at a growth rate higher than a certain level, $\hat{\gamma} > \frac{1}{\alpha_3}(\frac{1}{1-\kappa} - \beta) + \beta$, and thus, has a high inflation rate in equilibrium. Moreover, the parameter region $\hat{\gamma}$ gets higher when cryptocurrency becomes less acceptable or more costly to use (e.g., $\alpha_3 \downarrow$ or $\kappa \uparrow$). In this set-up, even if cryptocurrency is inferior in production costs and degrees of acceptability in decentralized markets, it can still coexist with fiat money—an asset that is more acceptable and costless to produce—when appropriate monetary policy is implemented.

[36] Appendix I presents the detailed equilibrium conditions under each special case in the two-currency model.

5.1.3. **Steady States and the Laffer Curve**

When fiat money competes with a private currency that is costly to produce, the monetary policy is constrained, thereby affecting the seigniorage earnings of the government. This point can be illustrated through the Laffer curve and its changes with the introduction of cryptocurrency. Following Ljungqvist and Sargent (2000), the Laffer curve for the inflation tax can be derived as:

$$z_m(\gamma)(1-\frac{1}{\gamma}).$$

Consider an economy without cryptocurrency—only fiat money is supplied as the medium of exchange. In this setting, the equilibrium real balance $z_m(\gamma)$ is determined by

$$\frac{\gamma-\beta}{\sigma\beta}=\frac{u'\circ\omega^{-1}(\beta\frac{z_m}{\gamma})}{\omega'\circ\omega^{-1}(\beta\frac{z_m}{\gamma})}-1.$$

Following Nosal and Rocheteau (2011), the functional forms are set to $u(q)=\frac{q^{1-a}}{1-a}$ with $a<1$ and $\omega(q)=q$, and the parameter values are summarized in Table 2. Figure 1 displays the Laffer curve and plots the government's seigniorage earnings as a function of γ.[37]

As shown in Figure 1, seigniorage increases with inflation until the inflation rate reaches γ^*, and then it decreases as the rate rises. The Laffer curve captures the tradeoffs faced by the government, which can benefit from inflation through increasing seigniorage earnings. However, as inflation rises beyond a certain level, the purchasing power of fiat money falls, thereby discouraging agents from holding it and decreasing seigniorage. As a result, there exists a level of money growth rate γ^* that maximizes the steady-state seigniorage.

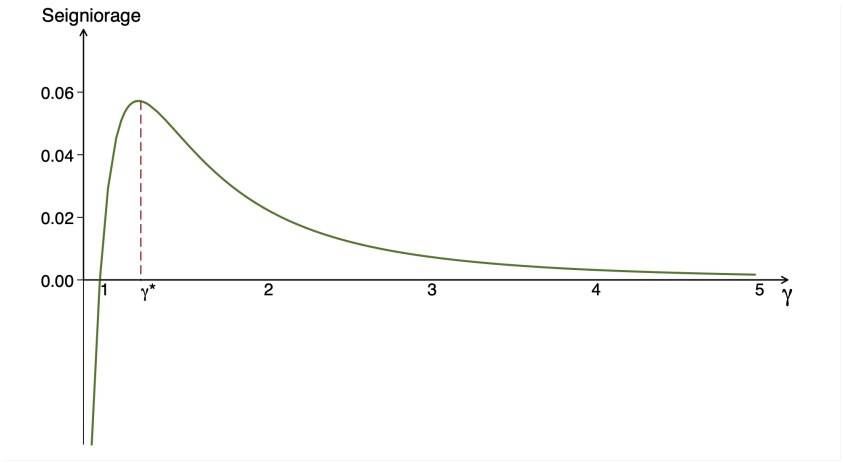
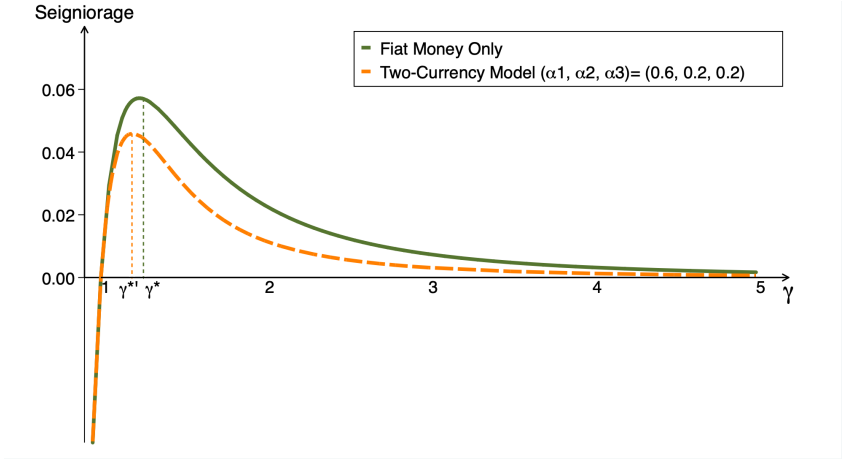


Figure 1. The Laffer Curve in Fiat Money Model

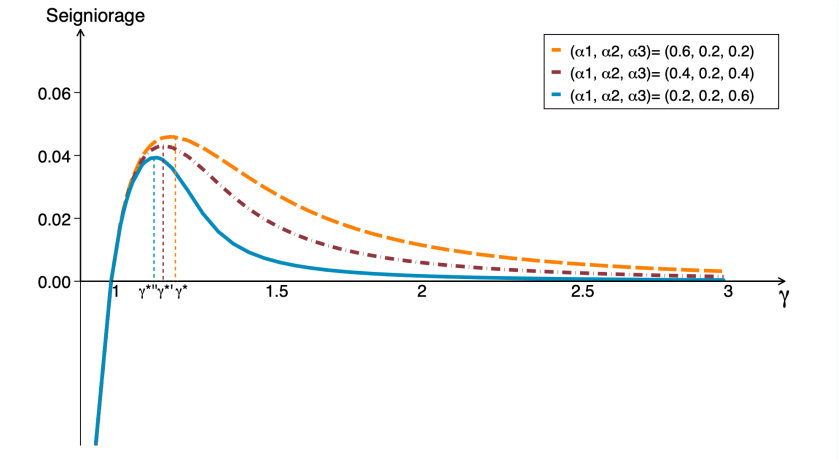
[37]See Appendix H for details on deriving the equilibrium of the fiat money-only economy and the Laffer curve.

Next, consider an economy with both fiat money and cryptocurrency. As described in Section 4, agents have a probability of entering the market where cryptocurrency is accepted alongside with fiat money. The equilibrium real balances, z_m and z_c, are jointly determined by (36) and (37) from Proposition 2. For example, if we apply the same functional forms and parameter values as above and set the probabilities of entering each market to $(\alpha_1, \alpha_2, \alpha_3) = (0.6, 0.2, 0.2)$, the Laffer curve in the two-currency economy is plotted in Figure 2 (a).

Compared to the fiat money economy, the Laffer curve in the two-currency model is lower, with its peak shifted to the left. Consequently, the seigniorage-maximizing level of money growth rate, γ^*, falls, and seigniorage earnings decrease, with the emergence of substitution between the two currencies. These results suggest that the existence of cryptocurrency constrains the monetary policy.



(a) Fiat Money Only vs. With Cryptocurrency



(b) Effects of Changing $\alpha_1, \alpha_2, \alpha_3$

Figure 2. The Laffer Curve in Two-Currency Model

Moreover, as more of the market where only fiat money is accepted shifts to one where both currencies can be accepted, e.g., $(\alpha_1, \alpha_2, \alpha_3)$ changes to $(0.4, 0.2, 0.2)$ and to $(0.2, 0.2, 0.6)$, the reduced market size for fiat money and the growth of substitution between currencies cause the Laffer curve to shrink further, as Figure 2 (b) displays. In other words, the larger the market size in which both currencies can be accepted, the lower the seigniorage-maximizing fiat money growth rate and the fewer seigniorage earnings when inflation rises.

The strategic interaction among money issuers has been studied in the literature. For instance, Zhu and Hendry (2019) model a policy-setting game between the government and E-money issuer. Zhang (2014) studies the dynamic policy game between two fiat money authorities and generates an inflation Laffer curve, capturing the tradeoffs faced by policymakers. My analysis contributes to the literature by clarifying how the introduction of cryptocurrency constrains the monetary policy. This is done via analysis of Laffer curves. Unlike fiat money and other private monies, the growth rule of cryptocurrency is not set by an issuer but endogenously determined by the production decisions of private agents.

Table 2: Parameter Values in Plotting Laffer Curves

	Figure 1	Figure 2a		Figure 2b		
	(1)	(2)	(3)	(4)	(5)	(6)
a	0.5	0.5	0.5	0.5	0.5	0.5
β	0.95	0.95	0.95	0.95	0.95	0.95
σ	0.5	0.5	0.5	0.5	0.5	0.5
κ	N/A	N/A	0.2	0.2	0.2	0.2
α_1	1	1	0.6	0.6	0.4	0.2
α_2	0	0	0.2	0.2	0.2	0.2
α_3	0	0	0.2	0.2	0.4	0.6

Columns 1 and 2 report parameter values in plotting the green curve in Figures 1 and 2 (a). Columns 3 and 4 report the values in plotting the orange curve in Figure 2. Columns 5 and 6 report those values in plotting the red and blue curves, respectively, in Figure 2 (b).

5.2. Implication

The existence of cryptocurrency restricts the inflation rate of fiat money. Specifically, in the economy where cryptocurrency is more acceptable in decentralized markets, fiat money has to maintain sufficiently low inflation in order to be valued and circulating in equilibrium; while in the economy where fiat money is more acceptable, cryptocurrency will be valued as well when the inflation rate of fiat money is above a certain level.

Should the government ban cryptocurrency? It depends on the acceptability of cryptocurrency in decentralized markets and the government's ability to commit to maintaining the targeted fiat money growth rule. Because cryptocurrency is costly to produce, banning cryptocurrency can clearly save the resources used in its production, i.e., $c(\delta, M^c)$. However, it may worsen the total welfare of the economy. One reason for this is that, in the absence of cryptocurrency, agents would only trade using fiat money in decentralized markets, thereby missing out on the trade surplus in DM2, where only cryptocurrency is accepted, s.t. $-\alpha_2[u(q_2) - \omega(q_2)]$, where $q_2 = \omega^{-1}(\beta z_c(1-\kappa))$. In that case, there would also be welfare changes from trade surplus in DM3 where both currencies are accepted, s.t. $\alpha_3[u(q_3^{'}) - \omega(q_3^{'})] - \alpha_3[u(q_3) - \omega(q_3)]$, where $q_3^{'} = \omega^{-1}(\beta\frac{z_m}{\gamma})$ and $q_3 = \omega^{-1}(\beta\frac{z_m}{\gamma} + \beta z_c(1-\kappa))$. In other words, if the government tends to overissue fiat money, there would be additional welfare loss from consuming less output.

In addition, competing with cryptocurrency restricts the government's ability to over-issue fiat money. If the government can maintain sufficiently low inflation and cryptocurrency is not widely accepted, then banning cryptocurrency might be welfare-enhancing. There would be welfare gains from avoiding resource waste associated with the cryptocurrency production and consuming more output, which would outweigh the welfare loss from no trade surplus in DM2.[38] Efficient allocations in DM1 and DM3 can be achieved when the monetary policy follows the Friedman rule if cryptocurrency is banned. Otherwise, if the government tends to over-issue money, banning cryptocurrency would worsen the total welfare. There would be welfare loss in all decentralized markets: no trade surplus in DM2 and less trade surplus in DM1 and DM3 from consuming fewer DM goods. As cryptocurrency is consistent with zero inflation in a stationary monetary equilibrium, the government that tends to use the inflation tax would have a strong incentive to ban cryptocurrency.

6. Conclusion

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

I first develop a model of cryptocurrency only and incorporate profit-maximizing miners, who are able to produce cryptocurrency according to a costly technology. The production cost strictly increases in both the number of newly produced units and the existing nominal stock of

[38] 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.

money. Compared to fiat money economies—the inflation rate can be different from zero—and other types of private money economies—the inflation rate must necessarily be different from zero—the cryptocurrency economy has an advantage of being consistent with zero inflation, due to the shape of its production cost function.

I then extend my cryptocurrency-only model by adding fiat money and multiple decentralized markets to study the currency competition between cryptocurrency and fiat money. The two currencies can circulate in equilibrium regardless of their rates of return. Even if cryptocurrency is inferior in production costs and acceptability in decentralized meetings, cryptocurrency can coexist with fiat money, when appropriate monetary policy is implemented. Further, the substitution between the two currencies constrains the monetary policy and affect seigniorage earnings. As cryptocurrency is consistent with zero inflation in a stationary equilibrium, banning cryptocurrency would worsen the welfare of the economy, when the government tends to use the inflation tax.

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. It is also 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

L. Ljungqvist and T. Sargent. *Recursive Macroeconomic Theory, Second edition*. Massachusetts Institute of Technology, 2000.

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.

G. Rocheteau and R. Wright. Liquidity and asset-market dynamics. *Journal of Monetary Economics*, 60:275–294, 2013.

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.

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

Lemma A.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.*

[Proof of Lemma A.1]

Proof. Follow directly from (3) and the discussion in the text.

□

Lemma A.2. *The terms of trade (q_t, d_t) that solve problem (4) are given by:*

$$q_t(m_t^b) = \begin{cases} q^* & if \quad m_t^b \geq m_t^* \\ \hat{q}_t & if \quad m_t^b < m_t^* \end{cases} \qquad d_t(m_t^b) = \begin{cases} m_t^* & if \quad m_t^b \geq m_t^* \\ m_t^b & if \quad m_t^b < m_t^* \end{cases} \tag{A.1}$$

where $q^* = argmax\ [u(q_t) - \omega(q_t)]$, $m_t^* = \frac{\omega(q^*)}{\beta p_{t+1}(1-\kappa)}$, and $\hat{q}_t = \omega^{-1}(\beta p_{t+1}(1-\kappa)m_t^b)$. In addition, $\hat{q}_t^{'}(m_t^b) > 0$ and $\hat{q}_t < q^*$, $\forall m_t^b < m_t^*$.

[Proof of Lemma A.2]

Proof. According to (3), problem (4) can be simplified as follows:

$$\begin{aligned} \max_{q_t, d_t} \quad & u(q_t) - \beta p_{t+1}(1-\kappa)d_t \\ s.t. \quad & -\omega(q_t) + \beta p_{t+1}(1-\kappa)d_t \geq 0 \\ & d_t \leq m_t^b \end{aligned} \tag{A.2}$$

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

□

Lemma A.3. *The optimal cryptocurrency holdings of a typical buyer and seller must satisfy:*

$$\frac{p_t}{\beta p_{t+1}(1-\kappa)} - 1 \geq \sigma L(m_t^b) \qquad \text{“} = \text{”} \ if \quad m_t^b > 0 \tag{A.3}$$

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

$$-p_t + \beta p_{t+1}(1-\kappa) \leq 0 \qquad \text{“ = ” } \textit{if} \quad m_t^s > 0 \tag{A.4}$$

[Proof of Lemma A.3]

Proof. It results from taking the first-order conditions (F.O.C.) of (7)-(8) with respect to m_t^b and m_t^s, respectively. Equivalently, the optimal cryptocurrency holdings can be obtained by taking the F.O.C. of (3) with respect to m_t^j, such that

$$-p_t + V_t^{j'}(m_t^j) \leq 0 \qquad \text{“ = ” if } \; m_t^j > 0, \quad j \in \{b, s\} \tag{A.5}$$

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

The term $L(m_t^b)$ is a liquidity factor that captures the marginal payoff that a buyer can get from using cryptocurrency to purchase more DM output in the decentralized market instead of carrying it to the next centralized market. $L = 0$ when a buyer can afford q^*, and $L > 0$ otherwise. □

[Proof of Lemma 2.1]

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

$$-p_t + V_t^{'}(m_t^b) = 0 \tag{A.6}$$

Following Lemmas A.1 and A.2, the DM value function (5) can be rewritten as follows:

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

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

Then we obtain:

$$V'(m_t^b) = \begin{cases} \beta p_{t+1}(1-\kappa) & if \quad m_t^b \geq m_t^* \\ \beta p_{t+1}(1-\kappa) + \sigma\beta p_{t+1}(1-\kappa)[\frac{u'(\hat{q}_t(m_t^b))}{\omega'(\hat{q}_t(m_t^b))} - 1] & if \quad m_t^b < m_t^* \end{cases} \tag{A.7}$$

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

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

Then $V'(m_t^b) > 0$ and $V''(m_t^b) < 0,\ \forall m_t^b < m_t^*$. Therefore, $V(m_t^b)$ is concave $\forall m_t^b < m_t^*$, and there is a unique $m_t^b < m_t^*$ solving the problem (A.6), which is expressed as (9) according to (A.7).

□

[Proof of Lemma 2.2]

Proof. The miner's problem (11) can be solved by taking the F.O.C. with respect to $[\delta_t^i]$: $p_t - \frac{\partial c(\delta_t^i, M_{t-1})}{\partial \delta_t^i} \leq 0, \text{“}=\text{”}$ if $\delta_t^i > 0$. Under Assumption 2.2, $\frac{\partial c(\delta_t^i, M_{t-1})}{\partial \delta_t^i}$ is increasing in δ_t^i and M_{t-1}. Then we have $\delta_t^i = c_\delta^{-1}(\max\{p_t, c_\delta(0, M_{t-1})\})$ where $c_\delta = \frac{\partial c(\delta_t^i, M_{t-1})}{\partial \delta_t^i}$.

□

[Proof of Proposition 1]

Proof. Suppose there exists a stationary equilibrium in which price changes at a constant rate, s.t. $\frac{p_t}{p_{t+1}} = \frac{M_{t+1}}{M_t} = (1+\mu)$, where $\mu > -\kappa$ and $\mu \neq 0$. According to (1) and (13), the aggregate production of cryptocurrency Δ_{t+1} must satisfy:

$$c_\delta^{-1}(p_{t+1}) = (\mu + \kappa)M_t \tag{A.8}$$

Following Lemmas A.3 and 2.1, the aggregate demand of cryptocurrency, M_t^d, satisfies:

$$1 + \mu = \beta(1-\kappa)\{1 + \sigma[\frac{u' \circ \omega^{-1}(\beta p_{t+1}(1-\kappa)M_t^d)}{\omega' \circ \omega^{-1}(\beta p_{t+1}(1-\kappa)M_t^d)} - 1]\} \tag{A.9}$$

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.8) and (A.9) with $M_t = M_t^d$. Therefore, p_{t+1} and M_t do not change, which contradicts to the assumption that the price of cryptocurrency changes over time.

In stationary, $p_t M_t = p_{t+1}M_{t+1} = z^{ss}\ \ \forall t$, and $\frac{M_{t+1}}{M_t} = \frac{p_t}{p_{t+1}} = 1$. Following the cryptocurrency law of motion, $\Delta^{ss} = \kappa M^{ss}$. Combining it with the aggregate production (13), we have (15).

Next, following Lemmas A.3 and 2.1, the aggregate demand of cryptocurrency, M^d, satisfies:

$$\frac{1-\beta(1-\kappa)}{\sigma\beta(1-\kappa)} = [\frac{u' \circ \omega^{-1}(\beta p^{ss}(1-\kappa)M^d)}{\omega' \circ \omega^{-1}(\beta p^{ss}(1-\kappa)M^d)} - 1] \tag{A.10}$$

Under Assumption 2.1, $\frac{u'(q)}{\omega'(q)}$ goes to infinity as q approaches zero, and it equals 1 when $q = q^*$. Therefore, $\frac{u'(q_t)}{\omega'(q_t)}$ is decreasing in q_t for $q_t < q^*$. As a result, given the functional forms and parameters of the model, there exists a unique value of p^{ss} and M^{ss} satisfying both (A.10) and (15) with $M^{ss} = M^d$. Accordingly, there is a unique $z^{ss} = p^{ss}M^{ss}$ solving (14). Likewise, following Lemma A.2, there is a unique q^{ss} that solves (16). By construction, the above results constitute a unique stationary monetary equilibrium in which the price of cryptocurrency is constant.

□

A.2. No Production of Cryptocurrency

This section provides a special case to the stationary monetary equilibrium of a cryptocurrency-only economy in which there is no cryptocurrency production.

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

$$\frac{1-\beta}{\sigma\beta} = [\frac{u' \circ \omega^{-1}(\beta z^{ss})}{\omega' \circ \omega^{-1}(\beta z^{ss})} - 1] \tag{A.11}$$

$$q^{ss} = \omega^{-1}(\beta z^{ss}) \tag{A.12}$$

[Proof of Proposition A.1]

Proof. In stationary, the real balances are constant, and $\frac{M_{t+1}}{M_t} = \frac{p_t}{p_{t+1}} = 1-\kappa \ \forall t$. Following Lemmas A.3 and 2.1, the real balance z^{ss} satisfies (A.11). Under Assumption 2.1, there exists a unique $z^{ss} > 0$ that solves (A.11). Next, following Lemma A.2, the consumption of the DM good $q^{ss} < q^*$ can be uniquely determined by (A.12). By construction, the above results constitute a unique stationary monetary equilibrium in which the price of cryptocurrency changes at a constant rate. In equilibrium, the stock of cryptocurrency in circulation is the existing stock.

□

A.3. Non-Stationary Equilibria

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

Proposition A.2. *Under Assumptions 2.1 and 2.2, there exists a continuum of equilibria in which the values of cryptocurrency converge to zero.*

[Proof of Proposition A.2]

Proof. Following Lemma 2.1, the relation between values of cryptocurrency p_t and p_{t+1} can be written as $p_t = g(p_{t+1})$ in equilibrium, such as:

$$p_t = \beta(1-\kappa)p_{t+1}(1-\sigma) + \beta\sigma(1-\kappa)p_{t+1}[\frac{u^{'} \circ \omega^{-1}(\beta p_{t+1}(1-\kappa)M_t)}{\omega^{'} \circ \omega^{-1}(\beta p_{t+1}(1-\kappa)M_t)}] \tag{A.13}$$

Under Assumption 2.1, there exists a unique $p_t = g(p_{t+1})$, $\forall p_{t+1} \geq 0$. Clearly, (A.13) goes through the steady state points $(0,0)$ and (p^{ss}, p^{ss}) where $p^{ss} > 0$. Next, following Lagos and Wright (2003), I show that in the space (p_t, p_{t+1}), the phase line representing RHS of the (A.13) intersects the 45° line from below, s.t. $g'(p^{ss} \mid_{p^{ss}=0}) > 1$ and $g'(p^{ss} \mid_{p^{ss}>0}) < 1$.

According to the law of motion and the aggregate production for cryptocurrency, the aggregate money stock M_t satisfies $M_t = M_{t-1} + c_{\delta}^{-1}(\max\{p_t, c_{\delta}(0, M_{t-1})\})$. Using the Implicit Function Theorem, the implicit differentiation becomes:

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

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

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

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

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

□

Proposition A.2 shows that cryptocurrency is subject to a self- fulfilling prophecy, even under the existence of a monetary equilibrium with a stable price. For an initial cryptocurrency value less than its steady-state value, there exists an equilibrium path that the values of cryptocurrency depreciate and converge to zero. Along the inflationary equilibrium trajectory, the expected depreciating currency values lead the real balances of cryptocurrency to decline and converge to zero. In this situation, agents' beliefs about the depreciating value of cryptocurrency can be self-fulfilling.

A.4. Two-Currency Model

Lemma A.4. *The solutions to the terms of trade (q_t^{DM}, d_t^{DM}) in the decentralized market DM, $DM \in \{1,2,3\}$, are given by:*

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

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

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

[Proof of Lemma A.4]

Proof. According to (22), problems (25)-(27) can be simplified as follows.

$$\text{In DM1:} \quad \max_{q_t^1, d_t^{1,m}} \quad u(q_t^1) - \beta p_{t+1}^m d_t^{1,m} \tag{A.14}$$
$$s.t. \quad -\omega(q_t^1) + \beta p_{t+1}^m d_t^{1,m} \geq 0, \quad d_t^{1,m} \leq m_t^{m,b}$$

$$\text{In DM2:} \quad \max_{q_t^2, d_t^{2,c}} \quad u(q_t^2) - \beta p_{t+1}^c (1-\kappa) d_t^{2,c} \tag{A.15}$$
$$s.t. \quad -\omega(q_t^2) + \beta p_{t+1}^c (1-\kappa) d_t^{2,c} \geq 0, \quad d_t^{2,c} \leq m_t^{c,b}$$

$$\text{In DM3:} \quad \max_{q_t^3, d_t^{3,m}, d_t^{3,c}} \quad u(q_t^3) - \beta p_{t+1}^m d_t^{3,m} - \beta p_{t+1}^c (1-\kappa) d_t^{3,c}$$
$$s.t. \quad -\omega(q_t^3) + \beta p_{t+1}^m d_t^{3,m} + \beta p_{t+1}^c (1-\kappa) d_t^{3,c} \geq 0 \tag{A.16}$$
$$d_t^{3,m} \leq m_t^{m,b}, d_t^{3,c} \leq m_t^{c,b}$$

Similar to the cryptocurrency-only economy, if a buyer can afford q^* using the currencies that are accepted as payment methods in that decentralized market, then the buyer would pay for q^*, i.e., $d_t^{1,m} = m_t^{m*} = \frac{\omega(q^*)}{\beta p_{t+1}^m}$, $d_t^{2,c} = m_t^{c*} = \frac{\omega(q^*)}{\beta p_{t+1}^c (1-\kappa)}$, $(d_t^{3,m}, d_t^{3,c}) = (\hat{m}_t^{m,b}, \hat{m}_t^{c,b})$ s.t. $\omega(q^*) = \beta(p_{t+1}^m \hat{m}_t^{m,b} + p_{t+1}^c (1-\kappa)\hat{m}_t^{c,b})$. Otherwise, the buyer would spend all the currencies that can be used in that market to purchase the DM good.

More specifically, in DM1: $d^{1,m} = m_t^{m,b}, q_t^1 = \omega^{-1}(\beta p_{t+1}^m m_t^{m,b}) < q^*$; in DM2: $d^{2,c} = m_t^{c,b}, q_t^2 = \omega^{-1}(\beta p_{t+1}^c (1-\kappa) m_t^{c,b}) < q^*$; and in DM3: $(d_t^{3,m}, d_t^{3,c}) = (m_t^{m,b}, m_t^{c,b}), q_t^3 = \omega^{-1}(\beta p_{t+1}^m m_t^{m,b} + \beta p_{t+1}^c (1-\kappa) m_t^{c,b}) < q^*$, which implies that cryptocurrency and fiat money are perfect substitutes in DM3 in equilibrium, in the sense that agents are indifferent about the two currencies.

The DM output, $q_t^{DM}, DM \in \{1,2,3\}$, can be proved following Lemma A.2.

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

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

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

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

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

□

Lemma A.5. *The optimal currency portfolios for a buyer and seller must satisfy:*

$$[m_t^{m,b}] \quad \frac{p_t^m}{\beta p_{t+1}^m} - 1 \geq \alpha_1 \sigma L(p_{t+1}^m m_t^{m,b}) + \alpha_3 \sigma L(p_{t+1}^m m_t^{m,b} + (1-\kappa) p_{t+1}^c m_t^{c,b})$$
$$\text{“}=\text{”}\ \textit{if} \quad m_t^{m,b} > 0 \tag{A.17}$$

$$[m_t^{c,b}] \quad \frac{p_t^c}{\beta p_{t+1}^c (1-\kappa)} - 1 \geq \alpha_2 \sigma L(p_{t+1}^c (1-\kappa) m_t^{c,b}) + \alpha_3 \sigma L(p_{t+1}^m m_t^{m,b} + (1-\kappa) p_{t+1}^c m_t^{c,b})$$
$$\text{“}=\text{”}\ \textit{if} \quad m_t^{c,b} > 0 \tag{A.18}$$

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

$$[m_t^{m,s}] \quad -p_t^m + \beta p_{t+1}^m \quad \leq 0 \quad \text{“}=\text{”} \quad \textit{if} \quad m_t^{m,s} > 0 \tag{A.19}$$

$$[m_t^{c,s}] \quad -p_t^c + \beta p_{t+1}^c(1-\kappa) \quad \leq 0 \quad \text{“}=\text{”} \quad \textit{if} \quad m_t^{c,s} > 0 \tag{A.20}$$

[Proof of Lemma A.5]

Proof. The optimal currency portfolios for a buyer and seller can be obtained by taking the F.O.C. of (28)-(29) with respect to $[m^{m,j}]$ and $[m^{c,j}]$, $j \in \{b, s\}$. The term $L(\cdot)$ represents the liquidity premium. It equals to zero when buyers can afford q^* in a decentralized meeting, and is strictly greater than zero when buyers cannot afford q^*.

□

[Proof of Proposition 2]

Proof. In stationary, $p_t^k M_t^k = p_{t+1}^k M_{t+1}^k = z_k^{ss}, k \in \{m, c\}$. According to Proposition 1, the price of cryptocurrency must remain constant in a stationary monetary equilibrium. When $M_{t+1}^m = \gamma M_t^m$ and $M_{t+1}^c = M_t^c$, a stationary equilibrium in which $z_m > 0$ and $z_c > 0$ exists, so long as $\beta < \gamma < \bar{\gamma}$ and $0 < \hat{\mu}$, where $\bar{\gamma} = \beta\alpha_1\sigma L(0) + \frac{\alpha_3}{\alpha_2+\alpha_3}(\frac{1}{1-\kappa} - \beta) + \beta$ is obtained from (35) by replacing $\mu = 0$, and $\hat{\mu} = \beta(1-\kappa)\{\alpha_2\sigma L(0) + 1\} - 1$ is obtained from (34), given $\gamma \in (\beta, \bar{\gamma})$.

Following (1) and (13), the aggregate production of cryptocurrency satisfies $\Delta^{ss} = c_\delta^{-1}(p_c^{ss})$ and $\Delta^{ss} = \kappa M_c^{ss}$, which implies (38). Following (30)-(31), the real balances of the two currencies, z_m^{ss} and $z_c^{ss} = p_c^{ss} M_c^{ss}$, satisfy (36)-(37). Following Lemma A.4, the steady state consumption of the DM good in each decentralized market satisfies (39)-(41). Given the functional forms and parameters of the model, the equilibrium outcomes can be jointly determined by (36)-(42), under Assumptions 2.1 and 2.2. By construction, the above results constitute a stationary equilibrium in which both currencies are valued.

□

Appendix B. An Extension of Cryptocurrency Security

This section models the cryptocurrency security in the cryptocurrency-only economy as theft instead of loss in the main text. The difference between loss and theft is that loss means a fraction

of cryptocurrency holdings is gone for every agent. In contrast, theft means some agents lose a fraction of their cryptocurrency holdings, but other agents get those lost units, making the aggregate stock of cryptocurrency unchanged before the production. Then the new cryptocurrency law of motion becomes:

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

Since the miner's problem is the same as in the cryptocurrency-only model with cryptocurrency loss, the aggregate new cryptocurrency supplied in period t, Δ_t, satisfies (13).

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

B.1. ***Buyers and Sellers***

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

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

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

The above CM value functions can be rearranged as:

$$W^b_t(m^b_{t-1}) = p_t(1-\kappa)m^b_{t-1} + W^b_t(0) \tag{B.2}$$

$$W^s_t(m^s_{t-1}) = p_t(m^s_{t-1} + \kappa m^b_{t-1}) + W^s_t(0) \tag{B.3}$$

where $W^b_t(0) = \max_{m^b_t \in \mathbb{R}_+} -p_t m^b_t + V^b_t(m^b_t)$ and $W^s_t(0) = \max_{m^s_t \in \mathbb{R}_+} -p_t m^s_t + V^s_t(m^s_t)$. Similar to Lemma A.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^b_t and m^s_t units of cryptocurrency, respectively. The DM value functions are the same as (5)-(6). According to (B.2)-(B.3), the terms of trade are given by the solution to:

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

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

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

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

[Proof of Lemma B.1]

Proof. Everything follows the Proof of Lemma A.2.

□

Then the DM value functions can be expressed as:

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

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

Next, from (B.2)-(B.3), the optimal cryptocurrency holdings, m_t^b, m_t^s, are given by the solutions to:

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

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

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

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

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

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

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

B.2. Stationary Equilibrium

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

Proposition B.1. *Under Assumption 2.1, there is no stationary monetary equilibrium in which the price changes at a constant rate s.t.* $\frac{p_t}{p_{t+1}} = (1+\mu), \mu \neq 0$. *There exists a unique stationary monetary equilibrium, in which the price of cryptocurrency is constant. The equilibrium outcomes are characterized by:*

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

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

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

[Proof of Proposition B.1]

Proof. Suppose there is a set of variables that construct a stationary equilibrium in which the price changes at a constant rate s.t. $\frac{p_t}{p_{t+1}} = \frac{M_{t+1}}{M_t} = (1+\mu)$. Following (B.1) and (13), the aggregate production of cryptocurrency must satisfy:

$$c_\delta^{-1}(p_{t+1}) = \mu M_t \tag{B.15}$$

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

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

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

In stationary, $p_t M_t = p_{t+1} M_{t+1} = z^{ss}, \ \forall t$. According to (B.1), $\Delta_t = 0$. Then following the optimal cryptocurrency holdings conditions and market clearing for cryptocurrency, the real balance z^{ss} satisfies (B.12). Under Assumption 2.1, there is a unique z^{ss} solving (B.12). Then following Lemma B.1, the steady state consumption of the DM good, $q^{ss} < q^*$, is uniquely determined by (B.13). By construction, the above results constitute a unique stationary monetary equilibrium, in which the price of cryptocurrency is constant. In this equilibrium, no cryptocurrency is produced.

□

Appendix C. Alternative Private Money Economy

In this section, I consider an alternative private money economy in which the cost of producing an additional unit of money is independent of the aggregate nominal stock.

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

Assumption C.1. *The cost function of producing private money,* $c(\delta_t^i) : \mathbb{R} \to \mathbb{R}$*, is increasing, convex, and twice differentiable, s.t.* $\frac{\partial c(\delta_t^i)}{\partial \delta_t^i} > 0,\ \frac{\partial^2 c(\delta_t^i)}{\partial \delta_t^{i2}} > 0$*, and satisfies* $c'(0) = 0$*.*

Then the maximization problem of a typical miner in period t is written as follows and can be solved by taking the F.O.C.

$$\max_{\delta_t^i \geq 0} \quad p_t \delta_t^i - c(\delta_t^i) \tag{C.1}$$

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

$$\delta_t^i = c_\delta^{-1}(\max\{p_t, c_\delta(0)\}), \quad \textit{where} \quad c_\delta = \frac{\partial c(\delta_t^i)}{\partial \delta_t^i} \tag{C.2}$$

In this set-up, a miner's production decision only depends on the price of private money.

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

Further, the aggregate new cryptocurrency in period t, Δ_t, becomes:

$$\Delta_t = \int_0^1 \delta_t^i di = c_\delta^{-1}(\max\{p_t, c_\delta(0)\}) \tag{C.3}$$

C.1. Economy Without Currency Depreciation

Suppose the currency depreciation rate is zero as in the standard private money literature, see, Fernández-Villaverde and Sanches (2019). Then the net circulation of money in each period is

only determined by the newly produced units, such that:

$$M_t = M_{t-1} + \Delta_t, \quad \Delta_t \geq 0, \quad M_{-1} \text{ given.} \tag{C.4}$$

Proposition C.1. *Under Assumptions 2.1 and C.1 and given $\kappa = 0$, a stationary monetary equilibrium of private money is inconsistent with price stability.*

[Proof of Proposition C.1]

Proof. Suppose there is a stationary equilibrium with a stable price, s.t. $p_t = p_{t+1} = p^{ss} > 0$. Under Assumption C.1 and given (C.3), $\Delta_t = c_\delta^{-1}(p^{ss}) > 0$. It follows that, $M_{t+1} > M_t$ under price stability, which violates the requirement of a stationary equilibrium. Thus, the price of cryptocurrency cannot remain constant, and the monetary equilibrium necessarily has positive inflation.

□

Intuitively, in order to have an equilibrium with a stable price, the aggregate nominal stock of private money must be constant. However, given the new shape of the production cost function in Assumption C.1, $c'(0) = 0$, miners always have an incentive to produce additional new units of private money when the money is valued. Therefore, the aggregate money stock cannot remain constant given zero currency depreciation. Thus, the equilibrium consistent with price stability cannot be sustained. Further, we cannot have a deflationary equilibrium either because miners would produce more new units due to the high return on money. Thus, if I make the marginal production cost independent of the aggregate nominal stock of money in my model and set the currency depreciation rate to zero, a monetary equilibrium would necessarily have positive inflation. The result of Fernández-Villaverde and Sanches is correct in a version of my model with different assumptions about the production cost function and currency depreciation.

C.2. Economy With Currency Depreciation

Next, consider an economy in which the cryptocurrency is lost at a positive rate $\kappa > 0$. In this case, the monetary equilibrium of private money is consistent with price stability.

Proposition C.2. *Under Assumptions 2.1 and C.1, there is no stationary monetary equilibrium in which the price of private money grows at a constant rate. There exists a unique stationary*

monetary equilibrium in which the price of private money is constant. The equilibrium outcomes are characterized by:

$$\frac{1-\beta(1-\kappa)}{\sigma\beta(1-\kappa)} = [\frac{u' \circ \omega^{-1}(\beta z^{ss}(1-\kappa))}{\omega' \circ \omega^{-1}(\beta z^{ss}(1-\kappa))} - 1] \tag{C.5}$$

$$1 + \frac{1-\beta(1-\kappa)}{\sigma\beta(1-\kappa)} = \frac{u'(q^{ss})}{\omega'(q^{ss})} \tag{C.6}$$

$$\Delta^{ss} = c_{\delta}^{-1}(p^{ss}) = \kappa M^{ss} \tag{C.7}$$

[Proof of Proposition C.2]

Proof. Everything follows the Proof of Proposition 1, by replacing the production cost function with the one specified Assumption C.1.

□

If private money has a positive depreciation rate, there is no inflationary equilibrium. Even though the marginal cost is independent of the nominal money stock, decreasing currency values weaken miners' incentives to produce money in excess of depreciated currency. Therefore, the aggregate stock of private money cannot be increasing, which violates the requirement of an inflationary equilibrium. In this setting, the stationary equilibrium is consistent with a stable price, and miners would constantly create new units that replace the depreciated money in each period.

Appendix D. Exogenously Supplied Cryptocurrency

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

$$M_t^c = M_{t-1}^c + \Delta_t - \kappa M_{t-1}^c = (1 + \epsilon - \kappa) M_{t-1}^c \tag{D.1}$$

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

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

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

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

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

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

D.2. **Equilibrium**

Definition D.1. *Given γ and ϵ, an equilibrium is a set of decision rules in the centralized market $\{x_t^b, \mathbf{m}_t^b, x_t^s, \mathbf{m}_t^s\}_{t=0}^{\infty}$, 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 (D.2)-(D.3) and (23)-(24); $\{(q_t^1, d_t^{1,m}), (q_t^2, d_t^{2,c}), (q_t^3, d_t^{3,m}, d_t^{3,c})\}$ solve problems (25)-(27); as well as market clearing for centralized good, fiat money, and cryptocurrency, and the 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 $M_{t+1}^c = (1+\epsilon-\kappa) M_t^c$ where $1+\epsilon-\kappa > \beta(1-\kappa)$, and according to (30)-(31), the equilibrium conditions satisfy:

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

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

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

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

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

D.3. Coexistence

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

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

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

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

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

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

[Proof of Proposition D.1]

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

□

Appendix E. Miners Carry Currencies

In this section, I assume that miners are allowed to carry currencies.

E.1. Carry Cryptocurrency

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

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

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

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

$$p_t - c_\delta(\delta_t^i, M_{t-1}) \leq 0 \qquad \text{“}=\text{”} \quad \text{if} \quad \delta_t^i > 0 \tag{E.2}$$

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

From (E.2), a miner will produce $\delta_t^i = c_\delta^{-1}(\max\{p_t, c_\delta(0, M_{t-1})\})$ units of cryptocurrency in period t. From (E.3), a miner will not hold any newly produced units when $p_t > \beta p_{t+1}(1-\kappa)$. Therefore, in a stationary monetary equilibrium in which the prices of cryptocurrency remain constant, miners do not keep any newly produced units, $m_t^i = 0, \ \forall t$.

E.2. Carry Fiat Money

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

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

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

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

$$p_t^c - c_\delta(\delta_t^i, M_{t-1}^c) \leq 0 \quad \text{“}=\text{”} \quad \text{if} \quad \delta_t^i > 0 \tag{E.5}$$

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

From (E.5), a miner will produce $\delta_t^i = c_\delta^{-1}(\max\{p_t^c, c_\delta(0, M_{t-1}^c)\})$ units of cryptocurrency in period t. From (E.6), a miner will not hold any unit of fiat money when it is costly to carry, i.e.,

$p_t^m > \beta p_{t+1}^m$. As the stock of fiat money grows at $\gamma > \beta, m_t^{m,i} = 0$ in equilibrium, $\forall t$. Therefore, the equilibrium outcomes remain the same as those of the two-currency model in Section 4, in which miners are assumed not to carry fiat money.

Appendix F. An Example of the Cost Function

This section describes the equilibrium outcomes of the cryptocurrency-only economy with the production cost function, $c(\delta_t^i, M_{t-1})$, specified in Example 2.1.

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:

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

A miner's production decision in each period depends on the value and the stock of cryptocurrency. A miner will not produce any cryptocurrency if $p_t - DM_{t-1} \leq 0$. Further, the aggregate new cryptocurrency in period t, Δ_t, becomes:

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

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

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

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

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

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

[Proof of Proposition F.1]

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

□

Appendix G. Comparative Statics

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix H. Fiat Money Economy and the Laffer Curve

This section derives the stationary equilibrium of the fiat money-only economy and generate the Laffer curve. Fiat money is exogenously supplied according to a deterministic growth rate, and it is modeled in the same way as in Section 4. However, there is no competition with cryptocurrency, i.e., $\alpha_1 = 1, \alpha_2 = \alpha_3 = 0$, and thus, no miner's sector.

H.1. ***Environment***

The CM value functions for a typical buyer b and seller s are:

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

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

The DM problems for a typical buyer and seller are represented by:

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

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

In each decentralized match, the terms of trade are determined by a take-it-or-leave-it offer by a buyer. The optimal offer is given by the solution to:

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

Lemma H.1. *The solutions to the terms of trade (q_t, d_t) in the decentralized market are given by:*

$$(q_t, d_t) = \begin{cases} (q^*, \ \ m_t^{m*} = \frac{\omega(q^*)}{\beta p_{t+1}^m}) & if \ \ \beta p_{t+1}^m m_t^{m,b} \geq \omega(q^*) \\ (\omega^{-1}(\beta p_{t+1}^m m_t^{m,b}), \ \ m_t^{m,b}) & if \ \ \beta p_{t+1}^m m_t^{m,b} < \omega(q^*) \end{cases}$$

Following Lemma H.1, the optimal currency portfolios, $m_t^{m,b}, m_t^{m,s}$, are given by the solutions to:

$$W_t^b(m_{t-1}^{m,b}) = \max_{m_t^{m,b} \in \mathbb{R}_+} -(p_t^m - \beta p_{t+1}^m) m_t^{m,b} + \sigma[u(q_t(m_t^{m,b})) - \beta p_{t+1}^m d_t(m_t^{m,b})]$$
$$W_t^s(m_{t-1}^{m,s}) = \max_{m_t^{m,s} \in \mathbb{R}_+} -(p_t^m - \beta p_{t+1}^m) m_t^{m,s} + 0$$

Lemma H.2. *The optimal currency portfolios for a buyer and seller must satisfy:*

$$[m_t^{m,b}] \quad \frac{p_t^m}{\beta p_{t+1}^m} - 1 \geq \sigma L(p_{t+1}^m m_t^{m,b}) \quad \text{“}=\text{”} \textit{ if } \quad m_t^{m,b} > 0$$
$$\textit{where } L(X) = \begin{cases} 0 & \textit{if} \quad \beta X \geq \omega(q^*) \\ \{\frac{u'}{\omega'} \circ \omega^{-1}(\beta X) - 1\} > 0 & \textit{if} \quad \beta X < \omega(q^*) \end{cases}$$
$$[m_t^{m,s}] \quad -p_t^m + \beta p_{t+1}^m \leq 0 \quad \text{“}=\text{”} \quad \textit{if} \quad m_t^{m,s} > 0$$

The term $L(\cdot)$ represents the liquidity premium. It equals to zero when buyers can afford q^* in a decentralized meeting, and is strictly greater than zero when buyers cannot afford q^*.

H.2. Equilibrium

Definition H.1. *Given γ, an equilibrium is a set of decision rules in the centralized market $\{x_t^b, m_t^b, x_t^s, m_t^s\}_{t=0}^\infty$, the terms of trade in the decentralized market $\{q_t, d_t\}_{t=0}^\infty$, and sequences of values of fiat money $\{p_t^m\}_{t=0}^\infty$, s.t. $\forall t \geq 0$: the CM and DM maximization problems are solved, and market clearing conditions for centralized good and fiat money are satisfied.*

Proposition H.1. *Given γ and $\alpha_1 = 1$, and under Assumption 2.1, there exists a stationary equilibrium in which fiat money are valued, and in which the price of fiat money changes at a constant rate s.t. $p_{t+1}^m = \frac{1}{\gamma} p_t^m$, so long as $\beta < \gamma < \bar{\gamma} \equiv \beta\sigma L(0) + \beta$. The equilibrium outcomes are characterized by:*

$$\frac{\gamma - \beta}{\sigma\beta} = [\frac{u' \circ \omega^{-1}(\beta \frac{z_m}{\gamma})}{\omega' \circ \omega^{-1}(\beta \frac{z_m}{\gamma})} - 1] \tag{H.1}$$
$$q^{ss} = \omega^{-1}(\beta \frac{z_m}{\gamma}) \tag{H.2}$$

[Proof of Proposition H.1]

Proof. In stationary, the real balances are constant. Under Assumption 2.1, there exists a unique $z_m > 0$ that solves (H.1). Following Lemma H.1, $q^{ss} < q^*$ is uniquely determined by (H.2). By construction, the above results constitute a unique stationary monetary equilibrium.

□

H.2.1. The Laffer Curve

According to Ljungqvist and Sargent (2000), the Laffer curve can be derived as $z_m(\gamma)(1-\frac{1}{\gamma})$, where the equilibrium $z_m(\gamma)$ is determined by (H.1). Following Nosal and Rocheteau (2011), the functional forms are set to $u(q) = \frac{q^{1-a}}{1-a}$ with $a < 1$ and $\omega(q) = q$. Then the Laffer curve becomes

$$z_m(\gamma)(1-\frac{1}{\gamma}) = (\frac{\sigma\beta+\gamma-\beta}{\sigma\beta})^{-\frac{1}{a}}(\frac{\gamma}{\beta})^{\frac{a-1}{a}}(1-\frac{1}{\gamma}).$$

By plugging into the parameter values specified in Table 2, the Laffer curve is plotted in Figure 1(a), as shown in Section 5.1.3.

Appendix I. Special Cases in Two-Currency Model

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

I.1. Completely Segmented Markets

Suppose there are only two decentralized markets in the economy: DM1 and DM2, i.e., $\alpha_1, \alpha_2 \in (0,1),\ \alpha_1+\alpha_2 = 1$, and $\alpha_3 = 0$. That is, agents are only allowed to trade with fiat money in DM1 and trade with cryptocurrency in DM2. Then equilibrium outcomes (30)-(31) can be expressed as follows:

$$\begin{aligned} i_m &\geq \alpha_1\sigma L(\frac{z_m}{\gamma}) && \text{“}=\text{” if } z_m > 0 \\ i_c &\geq \alpha_2\sigma L(\frac{z_c(1-\kappa)}{1+\mu}) && \text{“}=\text{” if } z_c > 0 \end{aligned}$$

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

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

$$\frac{1-\beta(1-\kappa)}{\sigma\beta(1-\kappa)}=\alpha_2[\frac{u'\circ\omega^{-1}(\beta z_c(1-\kappa))}{\omega'\circ\omega^{-1}(\beta z_c(1-\kappa))}-1] \tag{I.2}$$

$$c_\delta^{-1}(p_c^{ss})=\kappa M_c^{ss} \tag{I.3}$$

$$q_1^{ss}=\omega^{-1}(\beta\frac{z_m}{\gamma}) \tag{I.4}$$

$$q_2^{ss}=\omega^{-1}(\beta z_c(1-\kappa)) \tag{I.5}$$

$$\Delta^{ss}=\kappa M_c^{ss} \tag{I.6}$$

[Proof of Proposition I.1]

Proof. Everything follows the Proof of Proposition 2 by replacing $\alpha_3=0$. Then, under Assumptions 2.1 and 2.2, a set of equilibrium outcomes can be uniquely determined using (I.1)-(I.6), given the functional forms and parameters of the model.

□

Since each currency is essential in some transactions, agents will hold both currencies to smooth consumption in two decentralized markets, so long as neither currency is too costly to carry, and there is a dichotomy between two currencies' sectors in the economy.

I.2. Inherent Advantage to One Currency

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

I.2.1. Inherent Advantage to Cryptocurrency

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

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

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

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

$$\frac{\gamma - \beta}{\sigma\beta} = \alpha_3 [\frac{u' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\kappa)))}{\omega' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\kappa)))} - 1] \tag{I.7}$$

$$\frac{1 - \beta(1-\kappa)}{\sigma\beta(1-\kappa)} = \alpha_2 [\frac{u' \circ \omega^{-1}(\beta z_c(1-\kappa))}{\omega' \circ \omega^{-1}(\beta z_c(1-\kappa))} - 1] + \frac{\gamma - \beta}{\sigma\beta} \tag{I.8}$$

$$c_\delta^{-1}(p_c^{ss}) = \kappa M_c^{ss} \tag{I.9}$$

$$q_2^{ss} = \omega^{-1}(\beta z_c(1-\kappa)) \tag{I.10}$$

$$q_3^{ss} = \omega^{-1}(\beta \frac{z_m}{\gamma} + \beta z_c(1-\kappa)) \tag{I.11}$$

$$\Delta^{ss} = \kappa M_c^{ss} \tag{I.12}$$

[Proof of Proposition I.2]

Proof. Everything follows the Proof of Proposition 2 by replacing $\alpha_1 = 0$. The parameter region $\bar{\gamma}$ is obtained from (35) with $\alpha_1 = \mu = 0$, and $\hat{\mu}$ is obtained from (34) given $\gamma \in (\beta, \bar{\gamma})$. Similarly, the equilibrium outcomes can be uniquely determined by (I.7)-(I.12), given the functional forms $u(\cdot), \omega(\cdot)$, and model parameters, under Assumptions 2.1 and 2.2.

□

Since cryptocurrency can be used as a payment method everywhere, agents will carry it to facilitate all kinds of transactions in decentralized markets, as long as it is not too costly to hold. In order to give agents enough incentive to carry fiat money as well, the rate of return on fiat money has to be sufficiently high, or the inflation rate sufficiently low, in the equilibrium with both currencies in circulation.

I.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. The equilibrium conditions (30)-(31) can be expressed as:

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

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

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

$$\frac{\gamma - \beta}{\sigma\beta} = \alpha_1 [\frac{u' \circ \omega^{-1}(\beta \frac{z_m}{\gamma})}{\omega' \circ \omega^{-1}(\beta \frac{z_m}{\gamma})} - 1] + \frac{1 - \beta(1-\kappa)}{\sigma\beta(1-\kappa)} \tag{I.13}$$

$$\frac{1 - \beta(1-\kappa)}{\sigma\beta(1-\kappa)} = \alpha_3 [\frac{u' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\kappa)))}{\omega' \circ \omega^{-1}(\beta(\frac{z_m}{\gamma} + z_c(1-\kappa)))} - 1] \tag{I.14}$$

$$c_\delta^{-1}(p_c^{ss}) = \kappa M_c^{ss} \tag{I.15}$$

$$q_1^{ss} = \omega^{-1}(\beta \frac{z_m^{ss}}{\gamma}) \tag{I.16}$$

$$q_3^{ss} = \omega^{-1}(\beta \frac{z_m^{ss}}{\gamma} + \beta z_c(1-\kappa)) \tag{I.17}$$

$$\Delta^{ss} = \kappa M_c^{ss} \tag{I.18}$$

[Proof of Proposition I.3]

Proof. In stationary, the real balance of each currency is constant. When $M^m_{t+1} = \gamma M^m_t$ and $M^c_{t+1} = M^c_t$, a stationary equilibrium in which $z_m > 0$ and $z_c > 0$ exists, so long as $\hat{\gamma} \leq \gamma < \bar{\gamma}$, where $\bar{\gamma} = \beta\alpha_1\sigma L(0) + \frac{1}{1-\kappa}$ is obtained from (35) with $\mu = \alpha_2 = 0$ and $\hat{\gamma} = \frac{1}{\alpha_3}(\frac{1}{1-\kappa} - \beta) + \beta$ is obtained from (34) with $\bar{\mu} > 0$. Following the Proof of Proposition 2 by replacing $\alpha_2 = 0$, there exists a unique set of equilibrium outcomes that satisfy (I.13)-(I.18), under Assumptions 2.1 and 2.2, and given fundamentals of the model.

□

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