Discussion Paper Series – CRC TR 224

Discussion Paper No. 549
Project C 03

Blockchain Congestion Facilitates Currency Competition

Maxi Guennewig[1]

May 2024

[1]University of Bonn, Email: mguennewig@uni-bonn.de

Support by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) through CRC TR 224 is gratefully acknowledged.

Blockchain Congestion Facilitates Currency Competition*

Maxi Guennewig†

April 17, 2024

Abstract

Blockchain capacity constraints induce congestion when many users want to transact at the same time, challenging the usability of cryptocurrencies as money. This paper argues that blockchain capacity constraints, coupled with the need to incentivize miners (validators) to maintain blockchain security, lead to low inflation outcomes when cryptocurrencies compete for user demand. If two coins are both used as medium of exchange, a low-inflation coin must experience higher congestion than a high-inflation coin; otherwise demand for the latter is zero. Coin issuers then strategically undercut each other's money growth rates to boost transaction demand, limiting the overall inflation rate of the economy. However, the equilibrium is necessarily inefficient given unrealized gains from trade due to congestion and the cost of maintaining blockchain security.

Keywords: Cryptocurrencies, currency competition, blockchain, inflation.

JEL Codes: E40, E42, E5.

*I would like to thank Lukas Altermatt, Yuliyan Mitkov, Cyril Monnet, Ricardo Reis, Daniel Sanches, Hugo van Buggenum, Harald Uhlig and Ariel Zetlin-Jones for helpful comments and conversations. Support from the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) through the CRC TR 224 (Project C03) is gratefully acknowledged.

†University of Bonn, Department of Economics. Adenauerallee 24-26, 53113 Bonn, Germany. E-mail: *mguennewig@uni-bonn.de*. Web: *www.mguennewig.com*.

1 Introduction

Economists have debated the feasibility as well as the costs and benefits of private currency competition for a long time, dating back to at least Hayek's *Denationalization of Money* (1976). The idea is that private money initiatives compete for demand by promising more price-stable currencies than their competitors. The arrival of many blockchain-operated currencies since the inception of Bitcoin in 2008 has thrust this issue into the forefront of discussion. However, the usability of blockchain currencies as money is called into question for two reasons.

First, the decentralized nature of the network induces capacity constraints. As an example, the Ethereum network adds transactions to its ledger roughly every 10 seconds; given the block size of around 12 MB, this corresponds to 10-15 transactions per second. The system is thus unable to process as many transactions as users may submit.

Second, preserving the security of such decentralized networks exacts substantial costs. In the case of Bitcoin and other blockchains employing Proof-of-Work protocols, the network participant who updates that state of the blockchain is determined based on computing power. Honest miners require ample amounts of computing power in order to make it prohibitively costly to attack the blockchain. In the case of Ethereum and other blockchains employing Proof-of-Stake protocols, validators must lock up their wealth—that is, stake their coins—in order to update the blockchain. Honest validators require the majority stake in order to ensure network security. Providing large amounts of computing power and locking up large amounts of wealth is economically costly.

In light of new blockchain technology and its apparent drawbacks, this paper sets out to revisit the fundamental question: does currency competition work? In particular, does the private provision of blockchain-operated coins lead to low inflation outcomes?

I address these questions in a modified version of the workhorse monetary model of Lagos and Wright (2005). At the heart of the model is the idea that some economic interactions require a medium of exchange. This role is fulfilled by many competing, intrinsically worthless coins which are operated on blockchains. Given their lack of intrinsic value, I assume that all coins are perfect substitutes.

I add two constraints on these blockchain-operated coins. First, each individual blockchain faces a capacity constraint: the probability that a given user's submitted transaction is verified

successfully depends on the total number of users who submit transactions for verification on the blockchain. More precisely, when more transactions are submitted to the blockchain than its capacity, some transactions cannot occur and gains from trade are not realized. Probabilistic transaction verification captures any nuisance to users caused by congestion in a reduced form, including delayed transaction verification and increases in transaction fees.[1] Total capacity across all blockchains is, in principle, sufficient to cover all potential transactions.

Blockchain capacity constraints induce a trade-off. Coin holders prefer media of exchange which offer price stability, i.e. low inflation rates, and allow for transaction verification when needed. Therefore, if one coin experiences congestion while another coin does not, it must be that high-congestion coin is also experiencing lower inflation. Otherwise, the demand for the congested blockchain's coin would fall to zero. Importantly, blockchain congestion requires that many users employ the blockchain-native coin in their transactions. Congestion is thus associated with high demand.

The second constraint captures the need to maintain the security of the blockchain. Miners (validators) receive block rewards from coin issuance, i.e. the blockchain's seigniorage income. This implies that a coin's price cannot fall below a certain threshold level for a given nominal coin issuance. Otherwise miners supply too little computing power (validators stake too few coins) to maintain blockchain security. The system becomes susceptible to attacks and fails to provide a medium of exchange.

Given the second constraint, I identify weak sufficient conditions such that coins with lower coin growth rates also experience lower inflation rates. If coins with low growth rates experience higher inflation rates than high-growth coins, then the market value of the low-growth coins must tend to zero. This is inconsistent with an equilibrium in which both coins fulfill the role of the medium of exchange. As time passes, the low-growth blockchain becomes unsecured and susceptible to attacks. All users sell the coin in anticipation, and its price immediately falls to zero. Thus, if two coins jointly circulate in the economy, low-growth coins experience low inflation rates.

An undercutting logic emerges in equilibrium. If two coins are used as media of exchange, setting the coin growth rate below another coin's growth rate boosts blockchain capacity utilization. As the relative inflation rate falls, the demand for transaction verification jumps upwards. Operators

[1] I model transaction fees that rise with capacity utilization explicitly in one of the extensions.

of blockchains with under-utilization then face strict incentives to undercut other blockchain's monetary policy in order to achieve capacity over-utilization, i.e. induce congestion. It is in this sense that blockchain congestion facilitates currency competition.

In equilibrium, coin growth rates and thus miner (validator) income are so low that the total capacity of all coins in circulation is insufficient to verify all desired transactions. That is, congestion occurs in equilibrium. The equilibrium thus features opposing welfare effects. First, lower coin growth rates and subsequent lower inflation rates invite larger coin balances. This raises the welfare of coin users whose transactions are verified. However, some gains from trade cannot be realized. This reduces the welfare of unsuccessful coin users. Furthermore, all coin users are subject to strictly positive inflation since miners (validators) must receive a strictly positive transfer from coin users in order to supply computing power (wealth). The need to maintain blockchain security thus has real welfare costs.

Note one important caveat to the reasoning above. Whether a coin is used as medium of exchange is an outcome of coordination. Consequentially, a model with a single fiat currency typically has many equilibria with two steady states, including one in which the currency is not valued (Obstfeld and Rogoff, 1983).[2] The problem runs even deeper in multi-currency economies, as one can construct many equilibria in which different subsets of currencies are valued (Fernández-Villaverde and Sanches, 2019). It is therefore impossible to determine the equilibrium set of coins in circulation, given private monetary policies, without making additional assumptions.

The natural, arguably most conservative assumption is to extend the relationship between coin growth rates and inflation rates from the indeterminate set of circulating coins to the full set of coins that could possibly circulate. I therefore assume that low coin growth coins are valued in equilibrium and experience low inflation rates. High coin growth rates are also valued in equilibrium and experience high inflation rates—unless these inflation rates are so high that users prefer to switch to low-inflation high-congestion blockchains. The price of high growth coins then falls to zero. Without such a refinement, it is straightforward to construct equilibria in which currency competition leads to high inflation outcomes. As an example, suppose coordination is such that a coin is only valued if its supply doubles every period. Clearly setting a money growth rate of 100% is then optimal, and currency competition does not work.

[2]The contribution of Obstfeld and Rogoff (1983) is to point out that one needs to make the rather extreme assumption of infinite negative utility in the non-monetary steady state in order to rule it out.

It is useful to contrast my results to a benchmark without blockchain capacity constraints and security costs as in Fernández-Villaverde and Sanches (2019). Importantly, without blockchain capacity constraints, all coins circulating as medium of exchange must feature the same inflation rate (Fernández-Villaverde and Sanches, 2019; Schilling and Uhlig, 2019; Benigno et al., 2022). If coins are perfect substitutes, then demand for a coin experiencing a relatively higher inflation rate than another coin must be zero. With inflation rates equalized, coin holders are indifferent between all coins in circulation. As a consequence, the equilibrium portfolio breakdown between coins as well as their relative prices are indeterminate, a result first obtained by Kareken and Wallace (1981). Then, taking coin prices as given, blockchain operators find it profitable to issue large amounts of coins whenever the price is strictly positive, inevitably inducing highly inflationary outcomes (Fernández-Villaverde and Sanches, 2019).

The model lends itself to many extensions. First, I add transaction fees which are weakly increasing in the degree of blockchain congestion and show that the results are robust. Second, I allow for blockchain applications other than providing a medium of exchange. In particular, I assume that a subset of blockchains acts as a registry of the ownership of digital assets. Then whenever assets are registered on the blockchain, the blockchain-native coin must be valued in equilibrium. Otherwise purchasing the asset would incur zero costs, which constitutes a clear arbitrage. In a similar vein, blockchain applications guarantee that high-growth coins experience high-inflation, as any path that takes the coin price of low-growth coins with assets registered on the corresponding blockchain to zero cannot be an equilibrium outcome. Blockchain applications therefore ensure currency competition.

Literature review. This paper is primarily related to the two literatures on currency competition and blockchain economics. I start by discussing the former.

The most closely related work is by Fernández-Villaverde and Sanches (2019) who conclude that competition among perfectly substitutable, intrinsically worthless currencies leads to inflationary outcomes. My paper not only provides a much more realistic description of blockchain currencies but also obtains very different results. Other papers discuss different types of competitors. Schilling and Uhlig (2019) focus on competition between a private money and government money. They also rediscover the result of Kareken and Wallace (1981), albeit in its stochastic form as in Manuelli and Peck (1990). Benigno et al. (2022) show that a global currency, which is perfectly substitutable with

government money, induces two outcomes. First, all monetary policies across countries in which private money circulates are synchronized. Second, if the global currency pays interest, then all monetary authorities are forced to compete by removing the opportunity cost of their own money, i.e. setting the interest rate on government bonds to zero. In Cong and Mayer (2022), governments compete with a cryptocurrency by introducing central bank digital currency. Guennewig (2024) analyzes currency competition among firms and the government, and characterizes conditions such that firms are incentivized to implement low inflation rates in order to boost product sales. Biais et al. (2023) investigate whether changes to Bitcoin usability and hacking risks explain Bitcoin returns relative to government fiat money. The authors find that these factors have little explanatory power, and conclude that speculation is the key source for return differentials.

Turning to blockchain economics, Huberman et al. (2021) find that the delay in transaction verification due to blockchain capacity constraints may bring unexpected benefits to users. Congested blockchains can credibly price discriminate—charging higher transaction fees to users with urgent needs to consume—when a centralized payment system without capacity constraints such as Visa does not face incentives to do so. Even if the decentralized system is the monopoly payment provider and transaction fees temporarily rise due to congestion, miner entry pushes down transaction fees down for all users. Pagnotta (2022) shows that the equilibrium relationship between blockchain mining and coin usage gives rise to multiplicities. High usage pushes up the coin price which induces miner entry, raising the security level of the network and thus justifying higher usage in the first place. The reverse logic however also applies, and a second low usage-low security equilibrium exists. My contribution vis-à-vis the above papers is to focus on inflation outcomes. I highlight that the apparent drawbacks of cryptocurrencies, namely blockchain capacity constraints and security costs, enable currency competition.

Many more papers focus on different aspects of blockchain economics. Biais et al. (2019) and Saleh (2021) discuss miner and validator incentives for Proof-of-Work and Proof-of-Stake consensus protocols, respectively. John et al. (2022) show that increases in blockchain capacity have different equilibrium effects for blockchains with PoW consensus protocols than for blockchains with PoS consensus protocols. Budish (2023) highlights that network participants trade off the stock benefit of attacking a blockchain against the flow benefit of maintaining its integrity. This leads to security issues if Bitcoin became sufficiently economically important. Garratt and van Oordt (2023) stress

that the fixed costs of specialized Bitcoin mining equipment, which loses their value after a successful attack, work against such security risks. Lehar and Parlour (2020) document that Bitcoin miners do not utilize the full block capacity in order to increase transaction fees, which is inconsistent with competitive mining. Prat and Walter (2021) show that the Bitcoin-USD price predicts the network's total mining capacity, and find that block rewards have been primarily used to invest into mining equipment. Hinzen et al. (2022) describe how the decentralized nature of the Bitcoin network necessarily leads to low levels of adoption. See John et al. (2021) for a recent survey of the literature.

Outline of the paper. Section 2 introduces the framework. Section 3 characterizes money demand and supply. Section 4 develops the equilibrium concept. The properties of the equilibrium are characterized in Section 5. Section 6 provides a benchmark model without blockchain constraints. Section 7 extends the framework to analyze blockchain transaction fees and the effect of blockchain applications on currency competition. Section 8 concludes.

2 Model

2.1 Framework

The economy consists of a large number of three types of agents: a unit mass of buyers, a unit mass of sellers, and a set $\mathcal{N}$ of entrepreneurs, where $|\mathcal{N}| = N \in \mathbb{N}$. All agents are infinitely lived. Time is discrete. There is no aggregate uncertainty. Each period consists of two subperiods. In the first subperiod, all agents meet and consume in a centralized market (CM). Entrepreneurs have the expertise to issue specific coins which cannot be counterfeited. Buyers and sellers also meet in decentralized markets (DM). Sellers produce a perishable good but do not want to consume. Buyers want to consume but have no ability to produce. Entrepreneurs neither consume nor produce in the DM.

In the decentralized market, buyers and sellers interact in pairwise meetings. Each buyer is matched with one seller in every period with probability one. Sellers produce the consumption good at unit marginal cost. Assume that buyers have full market power in the DM. Further assume that buyers and sellers are anonymous which rules out credit. Trade thus requires a medium of exchange.

The entrepreneurs' coins, which are transferred in exchange for goods, fulfill this exact role. Let $\phi_t^n \in \mathbb{R}_0^+$ denote the price of coin n at time t, and let $1 + \pi_{t+1}^n = \phi_t^n / \phi_{t+1}^n$ denote the corresponding inflation rate.[3] For simplicity, I assume that buyers must choose one coin for each transaction.[4]

Let $x_{j,t} \in \mathbb{R}$ denote the buyer j's net consumption of the CM good. Let $q_{j,t} \in \mathbb{R}_0^+$ denote their DM good consumption. The buyers' preferences are represented by the utility function

$$u^b(x_{j,t}, q_{j,t}) \;=\; x_{j,t} + u(q_{j,t})$$

where $u : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ is thrice continuously differentiable, strictly increasing and strictly concave, with $\lim_{q \to 0} u'(q) = \infty$, $\lim_{q \to \infty} u'(q) = 0$ and $u(0) = 0$.

Let $x_{i,t} \in \mathbb{R}$ and $q_{i,t} \in \mathbb{R}_0^+$ denote seller i's net consumption of the CM good and their DM production, respectively. Their preferences are represented by the utility function

$$u^s(x_{i,t}, q_{i,t}) \;=\; x_{i,t} - q_{i,t}$$

Finally, let $x_{n,t} \in \mathbb{R}$ denote the entrepreneur n's net consumption of the CM good. Preferences are represented by the utility function

$$u^n(x_{n,t}) \;=\; x_{n,t}$$

I assume that all coins are operated on a blockchain, which are decentralized systems operated by miners on blockchains employing Proof-of-Work (PoW) consensus protocols, or validators on blockchains employing Proof-of-Stake (PoS) consensus protocols. In this model, the entrepreneur is a stand-in for the group of miners or validators active on a given blockchain.

Let $M_t^{n,S} \in \mathbb{R}_0^+$ and $\mu_t^n \in [-1, \infty)$ denote the nominal supply and the corresponding growth rate of coin n at time t. Given the nature of blockchain protocols, I assume that entrepreneurs need to decide on the lifetime private money issuance at time-0.[5] In other words, the path of the coin

[3] Define $\mathbb{R}^+ = \{y \mid y \in \mathbb{R}, y > 0\}$ and $\mathbb{R}_0^+ = \{y \mid y \in \mathbb{R}, y \geq 0\}$.

[4] This assumption is readily microfounded. Suppose a transaction is only fully verified if it has been verified for all coins used in the transaction; if there is no verification on at least one blockchain involved, the whole transaction is not verified. With independent verification probabilities across blockchains, low congestion blockchains do not provide an insurance against failure of verification on high congestion blockchains.

[5] This assumption is justified given the great difficulty of changing blockchain protocols once a blockchain is operational. Attempts at changing the protocol incur the risk of hard forks, as seen in the Bitcoin Cash fork of 2017 (see Biais et al. (2023) for details). The Ethereum London hard fork is a rare example of a successful protocol change.

growth rate $\{\mu_t^n\}_{t\geq 0}$ is set at time-0. For simplicity, assume that each coin issuer sets a constant coin growth rate $\mu_t^n = \mu^n$ for all $t \geq 0$. The vector of private coin growth rates $\boldsymbol{\mu}$ is perfectly observed by all agents. Going into period 0, all coins $n \in \mathcal{N}$ have an initial supply of $M_{-1} \in \mathbb{R}^+$ outstanding.[6]

2.2 Social planner

The social planner maximises the equal-weighted sum of all agents' payoffs. Market clearing in centralized markets requires that

$$\int_0^1 x_{j,t} dj + \int_0^1 x_{i,t} di + \sum_{n\in\mathcal{N}} x_{n,t} \;=\; 0$$

and the period welfare $\mathcal{W}_t$ is therefore given by

$$\mathcal{W}_t \;=\; \int_0^1 u^b(x_{j,t}, q_{j,t}) dj + \int_0^1 u^s(x_{i,t}, q_{i,t}) di + \sum_{n\in\mathcal{N}} u^n(x_{n,t}) \;=\; \int_0^1 \left(u(q_{j,t}) - q_{j,t}\right) dj$$

Efficiency then requires $q_{j,t} = q^*$ for all $j \in [0,1]$ and $t \geq 0$, where q^* is characterized by $u'(q^*) = 1$.

2.3 Blockchain congestion

One frequent criticism of cryptocurrencies is their lack of scalability. In particular, their decentralized nature also limits their capacity to verify transactions (see, e.g. Hinzen et al., 2022). I capture blockchain capacity constraints by assuming that only a mass $\eta \in (0,1)$ of transactions can be verified in any DM on each blockchain. Since each transaction in the DM involves one buyer, this corresponds to a limit on the mass of buyers which can successfully use a given coin.

Let $h_t^n \in [0,1]$ denote the mass of buyers using coin n for transactions in the DM at time t. A blockchain is said to experience congestion whenever $h_t^n > \eta$. Let α_t^n denote the probability that a buyer j's transaction is verified. I assume that this probability is proportional to the total mass of

However, its primary purpose was to switch from a PoW protocol to a PoS protocol, not to change monetary policy.

[6]The real value of coins is determined in the time-0 CM given the buyers' demand. Thus, the initial *nominal* level of coins outstanding is irrelevant as long as it is strictly positive.

buyers using coin n whenever the blockchain is congested, and is given by:

$$\alpha_t^n = \begin{cases} \frac{\eta}{h_t^n} & \text{if } h_t^n \geq \eta \\ 1 & \text{otherwise} \end{cases} \tag{1}$$

Importantly, the probabilistic transaction verification captures any nuisance caused by congestion in a reduced form, including delayed transaction verification and increases in transaction fees.[7]

I assume that N is arbitrarily large. In particular, aggregate blockchain capacity is more than sufficient: $(N-1) \cdot \eta > 1$. This is warranted by the large number of cryptocurrencies in circulation.

2.4 Blockchain security

Blockchains are decentralized networks, and the network security relies on the actions of its honest participants. A blockchain is only safe from attacks if miners supply a sufficiently large quantity of computing power (PoW), or if validators lock up a sufficiently large part of their wealth (PoS). Importantly, the network participants only do so if they receive sufficiently large block rewards, i.e. income from newly issued coins.[8]

This relationship between block rewards and blockchain security is captured in a reduced form. I assume that the blockchain belonging to entrepreneur n is secure if and only if $x_t^n \geq A$ for all $t \geq 0$, where $A \in \mathbb{R}^+$ is a parameter capturing a potential attacker's computing power or wealth. I assume that, whenever the level of block rewards falls below A, then $\phi_t^n = 0$.[9]

At each time $t \geq 0$, the entrepreneur's flow budget constraint reads $x_t^n = \phi_t^n \big(M_t^{n,S} - M_{t-1}^{n,S}\big)$. Using the money market clearing condition $M_t^{n,S} = M_t^n$, and defining aggregate real coin n balances as $m_t^n = \phi_t^n M_t^n = \int_0^1 \phi_t^n M_{j,t}^n dj$, the budget constraint becomes $x_t^n = \frac{\mu^n}{1+\mu^n} m_t^n$. The security constraint is therefore given by:

$$\frac{\mu^n}{1+\mu^n} m_t^n \geq A \tag{2}$$

Equation (2) implies a strictly positive lower bound on the coin growth rate if real coin balances are bounded.

[7] See Section 7.1 for an extension with transaction fees that rise with capacity utilization.
[8] I also consider income from transaction fees in Section 7.1.
[9] A zero price is consistent with equilibrium; see the discussion around Equation (3) below.

I assume that the parameters for the blockchain capacity and security constraints are such that a monetary equilibrium may exist. Intuitively, if $\eta \to 0$, the transaction benefit from holding a coin is vanishingly small. Similarly if $A \to \infty$, then block rewards need to be infinitely high in order to maintain blockchain security. In both cases, buyers would optimally hold vanishingly small coin balances and, consequentially, Equation (2) could never be satisfied in equilibrium. I provide precise conditions in Section 3.2, making use of equilibrium conditions derived Section 3.1, that help ensure equilibrium existence.

This completes the set-up.

3 Money demand and supply

3.1 Money demand

Consider the problem of buyer j during the time-t CM. Let $M_{j,t}^n \in \mathbb{R}_0^+$ denote buyer j's (non-negative) balances in coin n. Let $W_{j,t}$ denote j's CM value function. $W_{j,t}^n$ and $V_{j,t}^n$ denote the CM and DM value functions conditional on purchasing coin $n \in \mathcal{N}$ in the CM, respectively. Suppose j enters the CM with some nominal money balance of $M \in \mathbb{R}_0^+$ in some coin $n' \in \mathcal{N}$.

Buyers choose to hold the coin associated with the highest payoff: $W_{j,t} = max\left\{W_{j,t}^n\right\}_{n\in\mathcal{N}}$. Conditional on choosing coin n, the Bellman equation is written as

$$W_{j,t}^n(M) \;=\; \underset{(x_{j,t},M_{j,t}^n)\in\mathbb{R}\times\mathbb{R}_0^+}{max} \; x_{j,t} + V_{j,t}^n\left(M_{j,t}^n\right)$$

subject to the budget constraint

$$x_{j,t} + \phi_t^n M_{j,t}^n \;=\; \phi_t^{n'} M$$

Plugging in, the Bellman equation becomes

$$W_{j,t}^n(M) \;=\; \underset{M_{j,t}^n\in\mathbb{R}_0^+}{max} \; \phi_t^{n'} M - \phi_t^n M_{j,t}^n + V_{j,t}^n\left(M_{j,t}^n\right)$$

and is thus linear in coin balances M. Let $D_{j,t} \in \mathbb{R}$ denote the nominal transfer to the seller. The

DM value function is written as

$$V_{j,t}^n\left(M_{j,t}^n\right) \;=\; \max_{(q_{j,t},\,D_{j,t})\in\mathbb{R}_0^+\times\mathbb{R}} \alpha_t^n\cdot\left[u(q_{j,t})+\beta W_{j,t+1}\left(M_{j,t}^n-D_{j,t}\right)\right] \;+\; (1-\alpha_t^n)\cdot\beta W_{j,t+1}\left(M_{j,t}^n\right)$$

$$\text{s.t.}\quad D_{j,t} \;\leq\; M_{j,t}^n$$

$$q_{j,t} \;\leq\; \beta\phi_{t+1}^n D_{j,t}$$

The first constraint states that the transfer cannot exceed the buyer's money balance. After transacting, the seller holds onto the transfer until the following period's CM. The second constraint therefore implies that the seller must receive a discounted transfer that, given next period's coin price, weakly exceeds their cost of production in this period. Together these constraints capture the need for a medium of exchange in the DM.

Optimally, buyers do not transfer more to the seller than necessary, and hence $q_{j,t}=\beta\phi_{t+1}^n D_{j,t}$. Using the linearity of the Bellman equation, the DM value function simplifies to

$$V_{j,t}^n\left(M_{j,t}^n\right) \;=\; \max_{q_{j,t}\in\mathbb{R}_0^+} \alpha_t^n\cdot[u(q_{j,t})-q_{j,t}]+\beta\left[\phi_{t+1}^n M_{j,t}^n+W_{j,t+1}(0)\right]$$

$$\text{s.t.}\quad q_{j,t} \;\leq\; \beta\phi_{t+1}^n M_{j,t}^n$$

Consumption conditional on successful transaction verification is then given

$$q_{j,t} \;=\; \begin{cases} q^* & \text{if}\quad q^* \;\leq\; \beta\phi_{t+1}^n M_{j,t}^n \\ \beta\phi_{t+1}^n M_{j,t}^n & \text{otherwise} \end{cases}$$

and the DM value function becomes

$$V_{j,t}^n(M) \;=\; \begin{cases} \alpha_t^n\left[u\left(q^*\right)-q^*\right]+\beta\left[\phi_{t+1}^n M_{j,t}^n+W_{j,t+1}(0)\right] & \text{if}\;\; q^* \;\leq\; \beta\phi_{t+1}^n M_{j,t}^n \\ \alpha_t^n\left[u\left(\beta\phi_{t+1}^n M_{j,t}^n\right)-\beta\phi_{t+1}^n M_{j,t}^n\right]+\beta\left[\phi_{t+1}^n M_{j,t}^n+W_{j,t+1}(0)\right] & \text{otherwise} \end{cases}$$

I should stress that I focus on equilibria in which money demand is bounded. Then, plugging

the expression for $V^n_{j,t}(M)$ into the Bellman equation, the equilibrium coin price satisfies

$$\phi^n_t \;=\; \begin{cases} \beta\phi^n_{t+1} & \text{if } \; q^* \;\leq\; \beta\phi^n_{t+1}M^n_{j,t} \\ \alpha^n_t \cdot u'(\beta\phi^n_{t+1}M^n_{j,t}) \cdot \beta\phi^n_{t+1} \;+\; (1-\alpha^n_t)\cdot\beta\phi^n_{t+1} & \text{otherwise} \end{cases} \tag{3}$$

If the cash constraint is not binding, real money demand is only bounded if $\phi^n_t = \beta\phi^n_{t+1}$. The cash constraint is binding whenever $\phi^n_t > \beta\phi^n_{t+1}$. Optimal coin demand conditional on using coin n for a binding cash constraint is then characterized by the first order condition. The price ϕ^n_t is the cost of purchasing one real unit of coin n. This cost is traded off against the marginal benefit, which consists of the marginal consumption benefit from an additional unit of DM-consumption with probability α^n_t at time t, and of the marginal consumption benefit from an additional unit of CM-consumption with probability $1-\alpha^n_t$.

Note two important implications of Equation (3). First, if $\phi^n_t = 0$ for one $t \geq 0$, then $\phi^n_t = 0$ for all $t \geq 0$. This is feasible in equilibrium since $\lim_{q\to 0} u'(q)\cdot q$ is zero.[10] Going forward, let $\mathcal{M}$ denote the set of valued coins: $\mathcal{M} = \{n \in \mathcal{N} \mid \phi^n_t > 0 \;\text{ for all }\; t \geq 0\}$.

Second, if the set $\mathcal{M}$ is non-empty, then all buyers hold positive coin balances and $\sum_{n\in\mathcal{M}} h^n_t = 1$. If the cash constraint is not binding, then $M^n_{j,t} > 0$ by definition. Suppose the cash constraint is binding. Each buyer has infinitesimal weight and takes prices ϕ^n_t and verification probabilities α^n_t for all coins $n \in \mathcal{M}$ as given. Since $\alpha^n_t > 0$ for all $h^n_t \leq 1$, it cannot be optimal for any $j \in [0,1]$ to set $M^n_{j,t} = 0$ for all $n \in \mathcal{M}$.

Define $\tilde{m}^n_{j,t} = \beta\phi^n_{t+1}M^n_{j,t}$. Using the optimality conditions, rewrite the Bellman equation to read

$$W^n_{j,t}(M) \;=\; \phi^{n'}_t M \;+\; \alpha^n_t \cdot \psi\left(\tilde{m}^n_{j,t}\right) \;+\; \beta W_{j,t+1}(0)$$

[10] Suppose $u(0) = 0$. Consider some $q_0 > 0$. Since u is strictly concave and continuously differentiable, we have

$$u(q) \leq u\left(q_0\right) + u'\left(q_0\right)\cdot(q - q_0)$$

for all $q \geq 0$. Noting that $u'\left(q_0\right) \geq 0$ for all $q_0 \geq 0$, consider $q = 0$ and rearrange:

$$0 \;\leq\; u'\left(q_0\right)\cdot q_0 \;\leq\; u\left(q_0\right)$$

The right-hand side tends to zero as $q_0 \searrow 0$, implying $\lim_{q_0\searrow 0} u'\left(q_0\right)\cdot q_0 = 0$.

where $\psi : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ with

$$\psi(\tilde{m}) \;=\; \begin{cases} u(\tilde{m}) - \tilde{m} \cdot u'(\tilde{m}) & \text{if } \; 0 \;\leq\; \tilde{m} \;<\; q^* \\ u(q^*) - q^* & \text{if } \; \tilde{m} \;\geq\; q^* \end{cases}$$

By the properties of the utility function, note that $\psi(0) = 0$. Also note that $\psi'(\tilde{m}) = -\tilde{m} \cdot u''(\tilde{m}) > 0$ if $\tilde{m} \in (0, q^*)$, and $\psi'(\tilde{m}) = 0$ if $\tilde{m} \geq q^*$. It follows that $\psi(\tilde{m}_{j,t}^n)$ is strictly increasing in $\tilde{m}_{j,t}^n > 0$ whenever the cash constraint is binding.

Buyers choose to hold the coin associated with the highest expected utility. Hence $W_{j,t}^n(m) = W_{j,t}^{n'}(m)$ is a necessary condition for two coins n and n' to be both valued; otherwise buyers only hold the coin n with $W_{j,t}^n(m) > W_{j,t}^{n'}(m)$. This necessary condition is equivalent to

$$\alpha_t^n \cdot \psi(\tilde{m}_{j,t}^n) \;=\; \alpha_t^{n'} \cdot \psi(\tilde{m}_{j,t}^{n'}) \tag{4}$$

I am now ready to state the first result of the paper.

Proposition 1. *Consider $n, n' \in \mathcal{M}$. Then $\pi_{t+1}^n > \pi_{t+1}^{n'}$ if and only if $\alpha_t^n > \alpha_t^{n'}$.*

Proof. To show that $\pi_{t+1}^n > \pi_{t+1}^{n'}$ if $\alpha_t^n > \alpha_t^{n'}$, suppose $\alpha_t^n > \alpha_t^{n'}$. Equation (4) necessitates that $\psi(\tilde{m}_{j,t}^n) < \psi(\tilde{m}_{j,t}^{n'})$. The properties of ψ imply that $0 < \tilde{m}_{j,t}^n < \tilde{m}_{j,t}^{n'}$, with $\tilde{m}_{j,t}^n < q^*$. This in turn implies that $u'(\tilde{m}_{j,t}^n) > u'(\tilde{m}_{j,t}^{n'})$ if the cash constraint is binding for both coins. Combining first order conditions then reveals that $\pi_{t+1}^n > \pi_{t+1}^{n'}$. If the cash constraint is not binding for coin n', then $u'(\tilde{m}_{j,t}^n) > u'(q^*) = 1$, and hence also $\pi_{t+1}^n > \pi_{t+1}^{n'}$.

To show that $\pi_{t+1}^n > \pi_{t+1}^{n'}$ only if $\alpha_t^n > \alpha_t^{n'}$, suppose $\alpha_t^n \leq \alpha_t^{n'}$ and follow the same steps to find that $\pi_{t+1}^n \leq \pi_{t+1}^{n'}$. □

Proposition 1 highlights a trade-off. Buyers find both low inflation rates as well as high verification probabilities desirable. If one coin in circulation experiences a lower inflation rate than another coin in circulation, it must be that verification on the low-inflation coin's blockchain is less likely to occur. Otherwise, no buyer would want to hold the high-inflation coin.[11]

[11]The trade-off is reminiscent of models of directed search. See Wright et al. (2021) for a survey of the literature. In such frameworks, sellers can charge different prices in equilibrium if they face capacity constraints and thus cannot serve all possible buyers. Sellers with lower prices than their competitors than experience demand exceeding their capacity; buyers consume with probability less than 1. Sellers with higher prices also face strictly positive demand as they offer higher probabilities of consumption to buyers in equilibrium. One can interpret the relative inflation rates

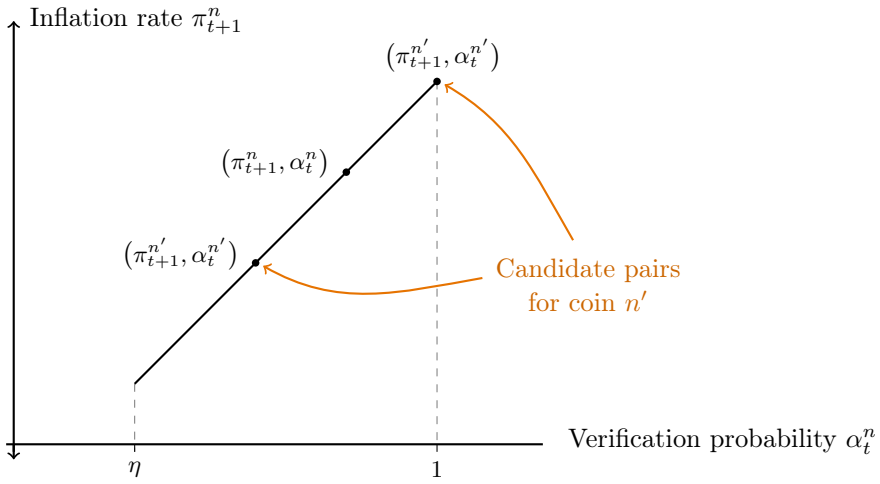

Figure 1: Illustration of Proposition 1.

Figure 1 illustrates this trade-off. Consider two coins $n, n' \in \mathcal{M}$. Then, for a given pair of inflation rate and transaction verification probability for coin n, the corresponding pair for coin n' must lie on the indifference curve. If coin n' is experiencing higher inflation, then the verification probability must be higher, and vice-versa.

Corollary 1. *If $\eta \geq 1$, then $\pi^n_{t+1} = \pi^{n'}_{t+1}$ for all $n, n' \in \mathcal{M}$.*

The corollary follows immediately from Proposition 1 if $\alpha^n_t = \alpha^{n'}_t = 1$ for all $n, n' \in \mathcal{N}$. Without blockchain capacity constraint, all transactions are verified on all blockchains with probability 1, regardless of the mass of buyers employing any coin. As a consequence, a necessary condition for two coins to both be valued in equilibrium is that they feature the same inflation rate. The indifference curve of Figure 1 only exists if blockchains are subject to capacity constraints.

Having established the relationship between inflation rates and verification probabilities for two coins $n, n' \in \mathcal{M}$, I now proceed to establish the corresponding relationship between inflation and coin growth rates. To this end, consider the following property of the utility function u.

Condition 1. $-\frac{u''(q)\cdot q}{u'(q)} < 1$ *for all* $q \in [0, q^*]$.

Condition 1 implies that $u'(q) \cdot q$ is strictly increasing in $q \in [0, q^*]$. It is a sufficient and sometimes necessary condition such that, ceteris paribus, real money demand is decreasing in the

of competing coins in this framework as the relative prices of consumption goods.

inflation rate (see e.g. Williamson, 2012). To illustrate, consider an economy with only one currency $n \in \mathcal{M}$. Set $\alpha_t^n = \alpha \in (0,1]$ and multiply Equation (3) with $M_{j,t}^n$ to obtain

$$m_{j,t}^n \equiv \phi_t^n M_{j,t}^n = \begin{cases} \tilde{m}_{j,t}^n & \text{if } q^* \leq \beta \phi_{t+1}^n M_{j,t}^n \\ \alpha \cdot u'(\tilde{m}_{j,t}^n) \cdot \tilde{m}_{j,t}^n + (1-\alpha) \cdot \tilde{m}_{j,t}^n & \text{otherwise} \end{cases}$$

Since $\tilde{m}_{j,t}^n$ is strictly decreasing in π_{t+1}^n, Condition 1 is a sufficient condition such that $m_{j,t}^n$ is strictly decreasing in π_{t+1}^n if $\alpha \in (0,1)$, and a necessary condition if $\alpha = 1$.

Indeed, Condition 1 is satisfied for many utility functions with the properties of u. For example, consider the class of utility functions exhibiting constant relative risk aversion: $u(q) = \frac{q^{1-\gamma}}{1-\gamma}$. The properties of u require $\gamma \in (0,1)$. Condition 1 then follows.

I am now ready to state the second result of the paper.

Proposition 2. *Consider two coins $n, n' \in \mathcal{M}$. Suppose Condition 1 is satisfied. If $\mu^n > \mu^{n'}$, then $m_t^n < m_t^{n'}$ for all $t \geq 0$.*

See Appendix A for the proof. To form an intuition, consider the equilibrium relationship between real money balances and inflation rates as an intermediate step. Three forces are at play. First, lower transaction verification probabilities lead buyers to reduce their real balances of the low-inflation coin. Second, more buyers hold the low-inflation coin, giving rise to the lower verification probabilities in the first place. It turns out that the latter effect dominates the former effect. Third, Condition 1 ensures that, ceteris paribus, real money balances are decreasing in the inflation rate. In sum, real money balances are larger for low-inflation coins, both due to the lower inflation rate and the larger mass of buyers.

To illustrate, suppose $\alpha_t^{n'} < \alpha_t^n$ which implies $h_{t+1}^{n'} > h_{t+1}^n$. Proposition 1 states that $\tilde{m}_{j,t}^{n'} > \tilde{m}_{j,t}^n$ and $\pi_{t+1}^{n'} < \pi_{t+1}^n$. Multiply both sides of Equation (3) by $h_t^n M_{j,t}^n$ and make use of definitions to obtain the time-t money demand:

$$m_t^n = \begin{cases} h_t^n \tilde{m}_{j,t}^n & \text{if } q^* \leq \tilde{m}_{j,t}^n \\ min\{h_t^n, \eta\} \cdot u'(\tilde{m}_{j,t}^n) \cdot \tilde{m}_{j,t}^n + (1-\alpha_t^n) \cdot h_t^n \tilde{m}_{j,t}^n & \text{otherwise} \end{cases} \tag{5}$$

Directly comparing m_t^n and $m_t^{n'}$ reveals that Condition 1 is a sufficient condition for $m_t^n < m_t^{n'}$ whenever $\pi_{t+1}^n > \pi_{t+1}^{n'}$.

To form an intuition about the relationship between real money balances and coin growth rates for valued coins, consider two coins $n, n' \in \mathcal{M}$. Suppose $\mu^{n'} < \mu^n$. Figure 2 fixes a path of the real coin balances of coin n with $\pi^n_{t+1} = \mu^n$ for all $t \geq 0$. The figure also illustrates two candidate paths of the real coin balances for coin n'. The first path for $m^{n'}_t$ supposes $\mu^{n'} = \pi^{n'}_{t+1}$ for all $t \geq 0$, implying that $m^n_t > m^{n'}_t$ for all $t \geq 0$. Since $m^n_{t+1} = \frac{1+\mu^n}{1+\pi^n_{t+1}} m^n_t$, real coin balances are constant for both coins $n, n' \in \mathcal{M}$.

The second path supposes $\pi^{n'}_{t+1} > \pi^n_{t+1}$ and thus $m^{n'}_t < m^n_t$. Since $m^n_{t+1} = \frac{1+\mu^n}{1+\pi^n_{t+1}} m^n_t$, coin n' features strictly lower aggregate real balances at time $t+1$ than coin n. But then coin n' must be experiencing a weakly higher inflation rate. As its coin supply continues to grow at a strictly lower rate than the supply of coin n, the relative aggregate real balances fall even further at time $t+2$. This process continues in every period going forward. Since real coin demand for n is bounded, it must be that real balances of coin n' that continue to fall—until they reach the threshold level at which the network becomes insecure and the coin's value immediately falls to zero.

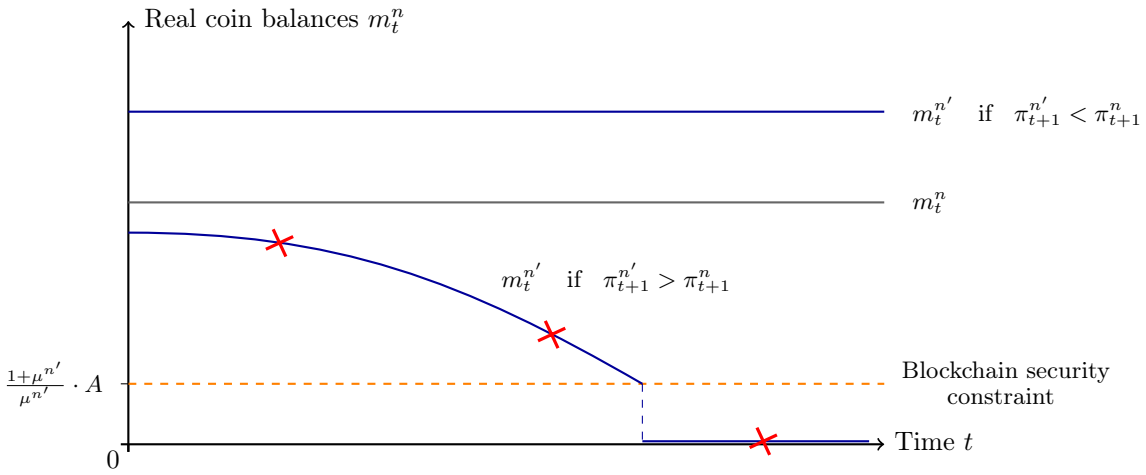

Figure 2: Candidate paths of real coin balances.

This cannot occur in equilibrium. Equation (3) highlights that coin prices must be zero on the entire equilibrium path if they fall to zero at some $t \geq 0$. Thus, coin n' could not have been valued in equilibrium in the first place, a contradiction. It follows that coins with lower coin growth rates must experience lower inflation rates in any equilibrium in which multiple coins are valued. Figure 3 illustrates the consequences of Proposition 2: if $\mu^{n'} < \mu^n$, then all coin n' candidate pairs

$\left(\pi_{t+1}^{n'}, \alpha_t^{n'}\right)$ with $\pi_{t+1}^{n'} > \pi_{t+1}^{n}$ are ruled out in equilibrium.

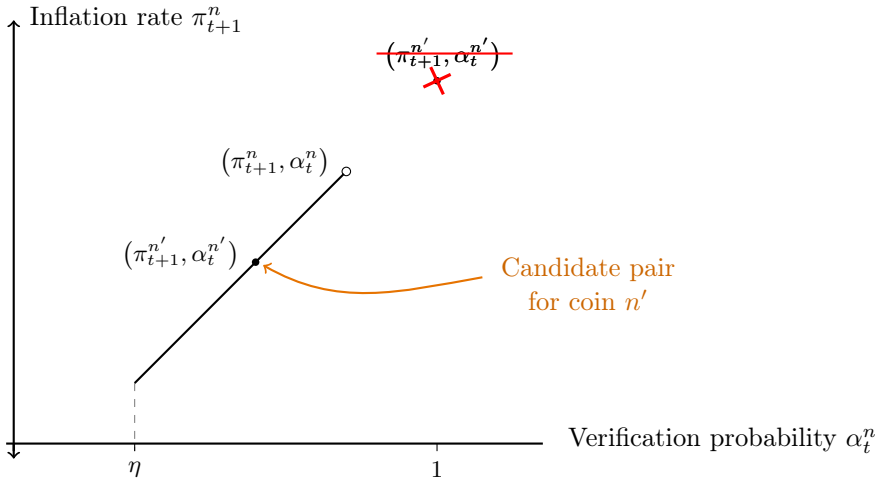

Figure 3: Illustration of Proposition 2.

Condition 1 is thus a weak sufficient condition such that higher coin growth rates translate into higher inflation rates if two coins circulate as media if exchange. Importantly, the relationship between relative coin growth and inflation rates must hold on the *entire* equilibrium path. Going forward, I will assume that Condition 1 is satisfied.

This concludes the discussion on money demand.

3.2 Money supply

Entrepreneurs choose their coin supply growth rate in order to maximise life-time payoffs U^n at time-0, given by

$$U^n = \sum_{t=0}^{\infty} \beta^t x_t^n = \sum_{t=1}^{\infty} \beta^t \frac{\mu^n}{1+\mu^n} m_t^n$$

In equilibrium, money demand is a function of monetary policy: $m_t^n = m_t^n(\boldsymbol{\mu})$. I make one joint restriction on the model parameters and the utility function that ensures the existence of a level of monetary policy such that both the blockchain security constraint and the equilibrium coin price condition can be satisfied.

Assumption 1. *There exists at least one $\mu \in \mathbb{R}^+$ for all $h \in [\eta, 1]$ that satisfies*

$$1 + \mu \;=\; \beta \cdot \frac{\eta}{h} \cdot u' \left(\frac{\beta \cdot A}{\mu \cdot h} \right) \;+\; \beta \cdot \left(1 - \frac{\eta}{h} \right) \tag{6}$$

Definition 1. *Let $\underline{\mu} : [\eta, 1] \to \mathbb{R}^+$ denote the function that assigns to each $h \in [\eta, 1]$ a value $\underline{\mu}(h)$ given by the lowest level of $\mu \in \mathbb{R}^+$ satisfying Equation (6). Let $\underline{\underline{\mu}}$ denote the function's minimum value over its domain.*

Equation (6) is a combination of the binding blockchain security constraint (Equation 2) and optimality conditions for coin holdings for a binding cash constraint (Equation 3), all in the steady state. Assumption 1 states that there exists a level of the coin growth rate for any degree of blockchain congestion such that money can be valued in equilibrium. Such a level may not exist if the blockchain constraints are prohibitively tight (that is, for high levels of A and low levels of η). Assumption 1 is warranted given the many cryptocurrencies circulating at a strictly positive price. Going forward, I shall use $\mu^n \geq \underline{\underline{\mu}}$ as constraint on the entrepreneurs' profit maximization problem.

Let $\mu^{n,*}$ denote the coin supply growth rate that solves entrepreneur n's maximization problem, given the other entrepreneurs' choice $\boldsymbol{\mu}^{-n}$:

$$\mu^{n,*} \;=\; arg\max_{\mu^n} \; U^n \Big(\mu^n, \big\{ m_t^n(\mu^n, \boldsymbol{\mu}^{-n}) \big\}_{t=0}^{\infty} \Big) \tag{7}$$

$$\text{s.t.} \quad \mu^n \;\geq\; \underline{\underline{\mu}}$$

However, the problem is not well-defined yet as the precise equilibrium relationship between private monetary policies and money demand, $\big\{ \boldsymbol{m}_t(\boldsymbol{\mu}) \big\}_{t=0}^{\infty}$, remains to be determined. Recall that relative coin inflation rates and transaction verification probabilities determine the buyers' money demand. However, entrepreneurs cannot directly choose their coin's inflation rate but can only attempt to affect it via the coin supply. Proposition 2 provides a ranking among real coin balances for all valued coins given their monetary policy, but it does not pin down the levels.

Furthermore, the results of the previous subsection do not determine which coins are valued in the first place. Additional assumptions are needed to determine the set $\mathcal{M}$. The following Lemma illustrates this need:

Lemma 1. *Suppose that $\mu^1 \leq \mu^2 \leq ... \leq \mu^{N-1} < \mu^N$. Then it must be that $\mathcal{M} \subset \mathcal{N}$.*

Proof. Suppose $\mathcal{M} = \mathcal{N}$, which implies that $h_t^1 \geq ... \geq h_t^{N-1} > h_t^N > 0$, with $\alpha_t^{N-1} < \alpha_t^N$ and thus $h_t^{N-1} > \eta$. Since $(N-1)\eta > 1$, it must be that $h_t^N = 0$ and hence $\phi_t^N = 0$. It follows that $\mathcal{M} \subset \mathcal{N}$, a contradiction. □

Lemma 1 shows that not all coins can be valued in equilibrium for all monetary policies. In the example above, which coins should not be valued in equilibrium? And if it's coin N, then does coin N become valued if the issuing entrepreneur undercuts some other entrepreneur $n < N$?

The problem runs even deeper, as illustrated by the following example. Suppose that buyers coordinate on valuing a given coin if and only if its coin growth rate is given by some arbitrary level, e.g. 100%. Clearly it is optimal to implement exactly this growth rate, as all other growth rates yield a zero payoff. Similarly it is always feasible to construct equilibria in which only a subset of coins can be valued, regardless of monetary policies.

For these reasons, I add further structure to the analysis in Section 4 below.

4 Equilibrium: Refinements & definition

Given the difficulty in determining which coins are valued and in pinning down the level of real coin balances, I apply two refinements to the set of possible equilibria. The first refinement helps determine the set $\mathcal{M}$:

Assumption 2 (R1). *If $\mu^n > \mu^{n'}$ implies that $m_t^n < m_t^{n'}$ for all $n, n' \in \mathcal{M}$ and all $t \geq 0$, then $\mu^n > \mu^{n'}$ implies the following for all $n, n' \in \mathcal{N}$ and all $t \geq 0$:*

a) $m_t^n \leq m_t^{n'}$, *and*

b) $m_t^n < m_t^{n'}$ *if $n' \in \mathcal{M}$ is consistent with equilibrium conditions, and*

c) $0 < m_t^n < m_t^{n'}$ *if $n, n' \in \mathcal{M}$ is consistent with equilibrium conditions.*

Proposition 2 established a relationship between the relative coin growth rates and the real level of coin balances when coins are valued. The refinement R1 extends this relationship from the set of valued coins to the set of all coins—as long as this is consistent with equilibrium conditions.

The refinement rules out arbitrary equilibria in which buyers only value coins that grow at a particular rate (e.g. 100%) or never value any coins that belong to some subset of $\mathcal{N}$. Instead,

as many coins as permitted by equilibrium conditions circulate as medium of exchange. Low coin growth coins are valued in equilibrium and experience low inflation rates. High coin growth rates are also valued in equilibrium and experience high inflation rates—unless these inflation rates are so high that users prefer to switch to low-inflation high-congestion blockchains, and the price of high growth coins falls to zero. With regards to the example of Lemma 1, the refinement ensures that coin N is not valued.

The second refinement provides clarification on the change in the level of real coin balances for marginal deviations in monetary policy:

Assumption 3 (R2). *Consider some monetary policy $\mu^n = \mu$ for all $n \in \mathcal{N}$ such that $\mathcal{M} = \mathcal{N}$ and $h_t^n \leq \eta$ for all $n \in \mathcal{N}$ and $t \geq 0$. Consider a deviation in monetary policy $\mu^n = \mu - \varepsilon < \mu$ for some $n \in \mathcal{M}$. I assume that*

$$\lim_{\varepsilon \searrow 0} m_{j,t}^n(\mu^n, \boldsymbol{\mu}^{-1}) \;=\; m_{j,t}^n(\boldsymbol{\mu}) \qquad \textit{and} \qquad \lim_{\varepsilon \searrow 0} \tilde{m}_{j,t}^n(\mu^n, \boldsymbol{\mu}^{-1}) \;=\; \tilde{m}_{j,t}^n(\boldsymbol{\mu})$$

where $m_{j,t}^n(\boldsymbol{\mu})$ and $\tilde{m}_{j,t}^n(\boldsymbol{\mu})$ denote the real money balances of buyer j as a function of monetary policy $\boldsymbol{\mu}$.

Lemma 2. *Assumption 3 is consistent with the equilibrium conditions.*

The proof is in Appendix B. By refinement R2, large swings in inflation rates (and thus individual coin balances) upon a marginal reduction in the growth rate of one coin do not occur. The refinement therefore rules out possible equilibria in which entrepreneurs fail to change their monetary policy in fear of inducing large upwards jumps in the inflation rate, rendering such changes unprofitable as buyers reduce their real money balances. Note that by Propositions 1 and 2, any swings in inflation rates would have to occur for *all* coins $n \in \mathcal{N}$ after marginal changes to one blockchain's monetary policy. Against this backdrop, Assumption 3 appears reasonable.

I am now ready to define the equilibrium. In the absence of any extrinsic and intrinsic aggregate uncertainty, I focus on perfect-foresight monetary equilibria. I also restrict attention to symmetric strategies for the entrepreneurs.[12]

Equilibrium definition. *A perfect-foresight monetary equilibrium consists of a non-empty set $\mathcal{M} \subseteq \mathcal{N}$, and an array $\{\alpha_t^n, h_t^n, \tilde{m}_{j,t}^n, m_t^n, \phi_t^n\}_{t \geq 0,\, j \in [0,1]}$ satisfying Equations (1)-(5) with $m_t^n < \infty$*

[12] See the end of Section 5 for a discussion of asymmetric strategies.

for each $n \in \mathcal{M}$, each $j \in [0,1]$, and all $t \geq 0$. Each entrepreneur $n \in \mathcal{N}$ sets $\mu^n = \mu^{n,*}$ as defined by Equation (7), given the refinements R1 and R2. Symmetry requires that $\mu^{n,*} = \mu^*$ for all $n \in \mathcal{N}$.

Going forward, I refer to any such equilibrium as 'monetary equilibrium.'

5 Equilibrium

Having defined the equilibrium concept, I am now ready to describe the key properties of every monetary equilibrium. For Propositions 3 - 5, suppose that a monetary equilibrium exists.

Proposition 3. *$\mu^n \leq \underline{\mu}(1)$ for all $n \in \mathcal{N}$.*

See Appendix C for the proof. Recall the definition of $\underline{\mu}(h)$ as the lowest level of $\mu \in \mathbb{R}^+$ satisfying the equilibrium coin pricing (Equation 3) for a binding blockchain security constraint (Equation 2) for some level $h \in [\eta, 1]$, all in steady state. Proposition 3 states that coin growth rates are bound from above by the lowest level that is consistent with a monetary equilibrium with only one operational blockchain.

The intuition is straightforward. If all coins are valued, then, given aggregate overcapacity, there exists at least one coin with a blockchain running below full capacity. This entrepreneur faces strict incentives to undercut other entrepreneurs to achieve full capacity utilization. If one coin is not valued, then the corresponding entrepreneur faces strict incentives to deviate to a coin growth rate which undercuts all other entrepreneurs and is consistent with a monetary equilibrium. Thus, if $\mu^n > \underline{\mu}(1)$ for all $n \in \mathcal{N}$, there always exists a profitable deviation to $\underline{\mu}(1)$.

Blockchain capacity constraints are key to obtain this result. The desire to undercut other entrepreneurs' coin growth rate arises as lower growth rates are associated with lower inflation rates, and lower inflation rates are associated with blockchain congestion. Since blockchain congestion requires transaction demand in excess of the blockchain capacity, it must be that lowering the coin growth rate boosts coin demand, the coin price, and thus the real value of newly issued coins.

Without blockchain capacity constraints, all coins must have equalized inflation rates in equilibrium. Section 6 below shows that the undercutting logic cannot arise without capacity constraints. Blockchain congestion therefore facilitates currency competition.

Proposition 3 highlights a welfare improving effect of blockchain congestion: low coin growth rates and subsequent low inflation rates improve the quality of the medium of exchange and thus

the levels of consumption and welfare. However, the private money arrangement on blockchain technology is inefficient. First, the blockchain capacity constraint induces welfare losses as congestion occurs in equilibrium:

Proposition 4. *If $\underline{\mu}(1) < \underline{\mu}(\eta)$, then $h_t^n > \eta$ for at least one $n \in \mathcal{M}$ for all $t \geq 0$.*

See Appendix D for the proof. If $\underline{\mu}(1) < \underline{\mu}(\eta)$, the same undercutting logic that limits the coin growth rates also leads to congestion in equilibrium. Entrepreneurs set monetary policy to such a low level that blockchain security can only be maintained if their blockchain experiences capacity over-utilization. The equilibrium thus cannot be efficient: with congestion, some gains from trade cannot be realized. The condition that $\underline{\mu}(1) < \underline{\mu}(\eta)$ is satisfied in the vast majority of model specifications; see the discussion around Condition 2 below.

Second, the need to generate strictly positive block rewards to maintain blockchain security implies that the inflation rate is inefficiently high:

Proposition 5. *There exists no monetary equilibrium with $q_{j,t} = q^*$ for all $j \in [0,1]$ and all $t \geq 0$.*

Proof. If $q_{j,t} = q^*$ for all $t \geq 0$ and $j \in [0,1]$, it must be that $q^* \leq \tilde{m}_{j,t}^n$ and hence $\pi_{t+1}^n = \beta - 1 < 0$ for all $n \in \mathcal{M}$ and all $t \geq 0$. Real coin balances are bounded and evolve according to $m_{t+1}^n = \frac{1+\mu^n}{1+\pi_{t+1}} m_t^n$. Since $\mu^n > 0$ for all $n \in \mathcal{M}$ in any monetary equilibrium by Equation (2), it cannot be that $\pi_{t+1}^n < 0$ for all $t \geq 0$ for any $n \in \mathcal{M}$. □

The need to generate income to the blockchain network participants implies that coins must be issued on the equilibrium path, leading to some level of inflation. Efficiency however requires that money has a strictly positive real return. That is, efficiency requires deflation. It follows that a monetary system operated on blockchains with endogenous security can never attain efficiency.

Given these properties of the equilibrium, does currency competition among blockchain-operated currencies work? Yes, and no. Blockchain capacity constraints give rise to low-inflation equilibria. Blockchain-operated currencies thus compete for demand by promising more price-stable currencies than their competitors. However, capacity constraints cause congestion in equilibrium. The limited transaction throughput leads to unrealized gains from trade, which can be interpreted more widely as any nuisance due to congestion, e.g. in the form of costly verification delays or transaction fees. Furthermore, the cost of maintaining blockchain security implies that the level of inflation is inefficiently high, a second reason efficiency cannot be achieved.

Propositions 3 - 5 assumed that an equilibrium exists and then described its properties. Condition 2 not only ensures that an equilibrium exists but also that its outcome is unique.

Condition 2. $\underline{\mu}(1) < \underline{\mu}(h)$ *for all* $h \in [\eta, 1)$.

Condition 2 states that the lowest possible coin growth rate that is consistent with a monetary equilibrium is the one when all buyers use the same blockchain: $\underline{\underline{\mu}} = \underline{\mu}(1)$. The following proposition characterizes the equilibrium outcome if the condition is satisfied:

Proposition 6. *Suppose Condition 2 is satisfied. In equilibrium it must be that* $\mu^n = \underline{\mu}(1)$ *for all* $n \in \mathcal{N}$*, with* $|\mathcal{M}| = 1$ *and* $\pi^n_{t+1} \leq \underline{\mu}(1)$ *for the single* $n \in \mathcal{M}$ *and all* $t \geq 0$.

Proof. With $\underline{\underline{\mu}} = \underline{\mu}(1)$, Proposition 3 implies that $\mu^n = \underline{\mu}(1)$ for all $n \in \mathcal{N}$ and hence $|\mathcal{M}| = 1$. Consider the single $n \in \mathcal{M}$ and suppose $\pi^n_{t+1} > \underline{\mu}(1)$ for one $t \geq 0$. Recall that $\sum_{n \in \mathcal{M}} h^n_t = 1$, implying $h^n_t = 1$. The first order condition for a binding cash constraint reads

$$1 + \pi^n_{t+1} \;=\; \beta \cdot \eta \cdot u'(\tilde{m}^n_{j,t}) + \beta \cdot (1 - \eta)$$

Then $\tilde{m}^n_{j,t} < \tilde{m}^n_j$, where $\tilde{m}^n_j$ is characterized by

$$1 + \underline{\mu}(1) \;=\; \beta \cdot \eta \cdot u'(\tilde{m}^n_j) + \beta \cdot (1 - \eta)$$

Recall that the definition of $\underline{\mu}(1)$ features a binding blockchain security constraint:

$$\frac{\underline{\mu}(1)}{1 + \underline{\mu}(1)} m^n \;=\; A$$

where m^n is the steady state level of money balances. Equation (5) implies that $m^n_t < m^n$ if $\tilde{m}^n_{j,t} < \tilde{m}^n_j$. Then

$$\frac{\underline{\mu}(1)}{1 + \underline{\mu}(1)} m^n_t \;<\; A$$

which is a contradiction to $n \in \mathcal{M}$. The claim follows. □

Intuitively, if $\underline{\mu}(1)$ is the lowest coin growth rate that is consistent with a monetary equilibrium, then all entrepreneurs set their monetary policy to this level. By the of definition $\underline{\mu}(1)$, only one coin can be valued in equilibrium. Furthermore, the blockchain security constraint is binding if

$\pi^n_{t+1} = \underline{\mu}(1)$. Since all buyers hold this coin in equilibrium, the corresponding blockchain experiences strong degrees of congestion. Inflation is bound from above by the coin growth rate. Otherwise, the blockchain security is violated as the buyers' real money balances fall to an insufficiently high level.

Indeed, Condition 2 is satisfied for many specifications of the model:

Lemma 3. *Define* $\tilde{\mu} = \lim_{\eta \to 1} \underline{\mu}(\eta)$. *If* $1 > u'\left(\frac{\beta A}{\tilde{\mu}}\right) + u''\left(\frac{\beta A}{\tilde{\mu}}\right) \cdot \frac{\beta A}{\tilde{\mu}}$, *then there exists some* $\underline{\eta} \in (0,1)$ *such that Condition 2 is satisfied whenever* $\eta \geq \underline{\eta}$.

See Appendix E for the proof. Lemma 3 highlights that Condition 2 is satisfied if the blockchain capacity is sufficiently big as long as $1 > u'\left(\frac{\beta A}{\tilde{\mu}}\right) + u''\left(\frac{\beta A}{\tilde{\mu}}\right) \cdot \frac{\beta A}{\tilde{\mu}}$. If $u(q) = \frac{q^{1-\gamma}}{1-\gamma}$, with $\gamma \in (0,1)$, the inequality simplifies to $\beta > (1-\gamma)(1+\tilde{\mu})$. Given the short-length of a period in this model, the discount factor β is close to one. The inequality is then satisfied if the coefficient of relative risk aversion is not too small relative to the lowest possible money growth rate consistent with a monetary equilibrium at a blockchain capacity of one.

Figure 4 shows the numerical computations of $\underline{\mu}(h)$ and its derivative with respect to h for the utility function $u(q) = \frac{q^{1-\gamma}}{1-\gamma}$. The left panel of Figure 4 depicts $\underline{\mu}(h)$ for different levels of blockchain capacity $\eta \in [0.08, 0.99]$, with $\gamma = 0.1$.[13] The right panel depicts $\frac{d\underline{\mu}(h)}{dh}$ for the same levels of η. The surface is red whenever the derivative is positive and Condition 2 is not satisfied. Note that $\underline{\mu}(h)$ is strictly decreasing in h, reaching its minimum at $\underline{\mu}(1)$, if η is sufficiently large. Figure 5 shows the corresponding computations for different levels of the coefficient of relative risk aversion $\gamma \in [0.1, 0.99]$, with $\eta = 0.08$. It turns out that Condition 2 is satisfied for most specifications of this utility function even for a low level of blockchain capacity.

Importantly, scaling solutions are being developed in order to increase blockchain capacity (Bertucci, 2020; Guasoni et al., 2023a,b; Cong et al., 2023). One example is the *Lightning Network*, which is a second-layer protocol built on top of Bitcoin's blockchain. It operates by creating payment channels between users on-chain that can execute transactions off-chain. If no direct channel between two users exists, then payments can be facilitated via existing third-party channels in the network. Divakaruni and Zimmerman (2023) show that the possibility to settle transactions off-chain reduces blockchain congestion, effectively increasing blockchain capacity.

The result highlights the importance of blockchain scaling solutions for equilibrium outcomes: if blockchain capacity increases up to a threshold, then Proposition 6 describes the unique equilibrium

[13] The fixed parameters are set to $A = 0.001$ and $\beta = 0.99$. Recall that $\underline{\mu}(h)$ is not defined for $h < \eta$.

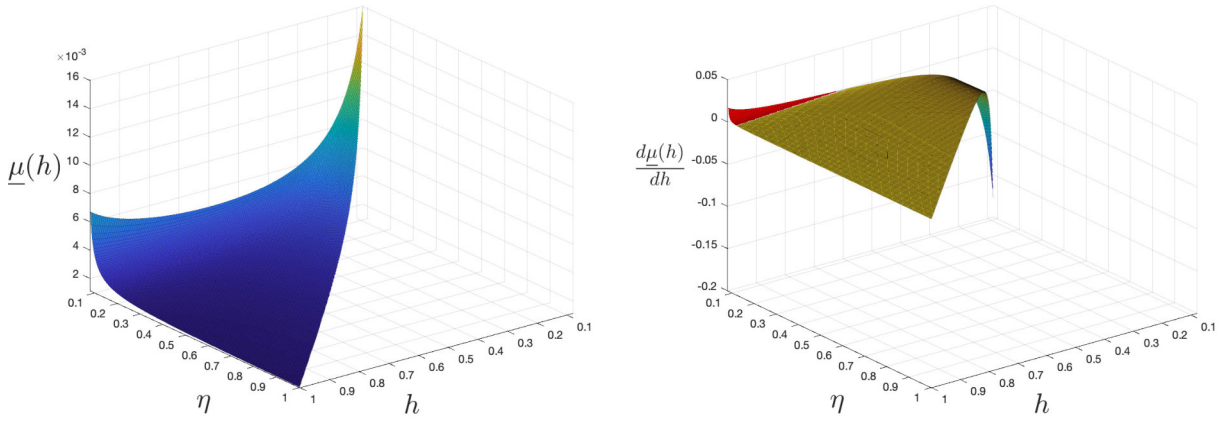

Figure 4: Numerical computations of $\underline{\mu}(h)$ and $\frac{d\underline{\mu}(h)}{dh}$ for different levels of η, with $\gamma = 0.1$.

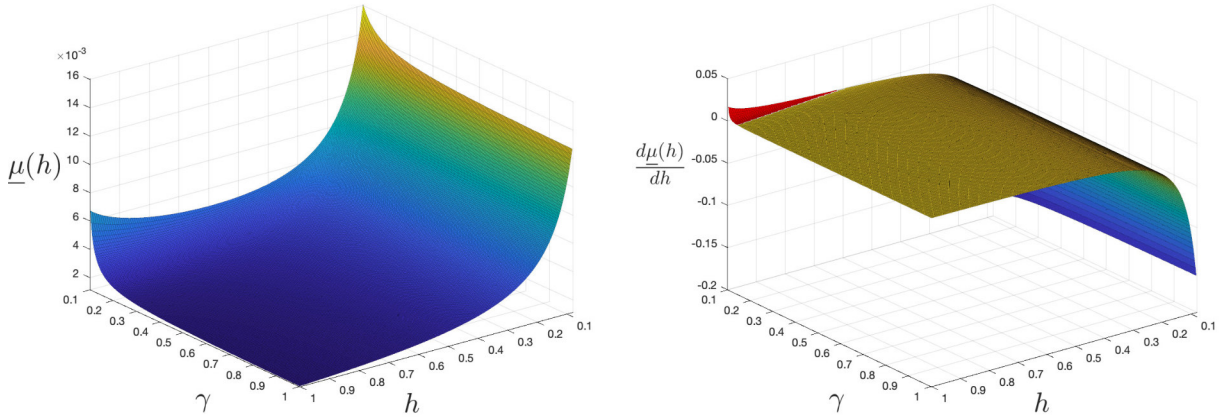

Figure 5: Numerical computations of $\underline{\mu}(h)$ and $\frac{d\underline{\mu}(h)}{dh}$ for different levels of γ, with $\eta = 0.08$.

outcome. However, by Corollary 1, the results of Propositions 3 - 6 hinge on limited capacity. If blockchain scaling solutions fully remove the capacity constraints, then the favourable results on currency competition no longer stand, as illustrated in Section 6 below.

Finally, Lemma 3 highlights that focusing on symmetric entrepreneur strategies is merely a simplification if the blockchain capacity is sufficiently large. Even in asymmetric strategies, entrepreneurs continue to face strict incentives to undercut other coins' money growth rates in order to boost demand. The equilibrium outcome of Proposition 6 thus stands.[14]

This concludes the main analysis.

[14]Note that the analysis of asymmetric strategies would require adjustments to the proofs of Lemma 2 and Propositions 3, 4 and 6.

6 Benchmark

It is useful to contrast these results to a benchmark without blockchain capacity and security constraints. This section demonstrates that the model rediscovers the result of Fernández-Villaverde and Sanches (2019) if individual blockchains have sufficient capacity to verify all transactions in the DM and are not subject to security risks. In other words, if $\eta \geq 1$ and $A = 0$, then currency competition leads to inflationary outcomes.

By Corollary 1, inflation rates are equalized for all coins $n \in \mathcal{M}$ with $\eta \geq 1$. With $A = 0$, the blockchain security constraint (Equation 2) is satisfied for any $m_t^n \geq 0$ if $\mu^n \geq 0$.[15] As all coins experience the same inflation rate, buyers are indifferent between them. Hence, any $h_t^n \in [0, 1]$ is an equilibrium outcome for all $n \in \mathcal{M}$. Consequentially, coin prices ϕ_t^n are indeterminate for any $n \in \mathcal{M}$ and entrepreneurs must take them as given. This is the indeterminacy result first obtained by Kareken and Wallace (1981) and central to the analysis in Fernández-Villaverde and Sanches (2019).

The following proposition highlights that currency competition in this benchmark leads to highly inflationary outcomes:

Proposition 7. *There exists no monetary equilibrium with $\phi_0^n > 0$ and $\mu^n < \infty$ for any $n \in \mathcal{N}$.*

See Appendix F for the proof. The intuition is simple. Taking prices as given, entrepreneurs find it optimal to issue large amount of coins whenever the price is strictly positive. With the money supply growing at a very high rate, the inflation rate of the valued coins must also be very high.

This result highlights the importance of the blockchain capacity constraints. Without blockchain congestion, all coins circulating as medium of exchange must feature the same inflation rate. Entrepreneurs then do not face incentives to lower their coin growth rate in order to boost demand for their coin.

The benchmark result mirrors the main result of Fernández-Villaverde and Sanches (2019) who also find that entrepreneurs issue large amount of coin but model the mining process with a strictly increasing cost of coin issuance. Since it is costless to issue coins in this framework, coin issuance here is unbounded.[16]

[15] Setting $\mu^n < 0$ rate yields negative payoffs to entrepreneurs and is strictly dominated by $\mu^n = 0$.

[16] Issuing new blockchain-operated coins is not necessarily costly. To illustrate, the block reward in the Bitcoin

One can consider two further benchmark models, each with only one of the constraints. Suppose first that only the blockchain capacity constraint applies: $\eta \in (0,1)$ but $A = 0$. Then the result of Proposition 2 does not hold: it becomes a valid equilibrium path for m_t^n to tend to zero as time progresses. Both paths illustrated in Figure 2 are consistent with equilibrium conditions. As a consequence, the refinement of Assumption 2 has no bite. It is then easy to construct an equilibrium with high coin growth rates, for example with a negative correlation between coin growth and inflation rates, which cannot be ruled out in equilibrium.

Suppose next that only the blockchain security constraint applies: $A \in \mathbb{R}^+$ but $\eta \geq 1$. By Corollary 1, all coins $n \in \mathcal{M}$ must feature the same inflation rate. Suppose $\mu^n < \mu^{n'}$. Real coin balances are bounded and evolve according to $m_{t+1}^n = \frac{1+\mu^n}{1+\pi_{t+1}} m_t^n$, and hence relative real coin balances satisfy

$$\frac{m_{t+1}^n}{m_{t+1}^{n'}} = \frac{1+\mu^n}{1+\mu^{n'}} \cdot \frac{m_t^n}{m_t^{n'}}$$

If both $m_t^n > 0$ and $m_t^{n'} > 0$, then it must be that $\lim_{s\to\infty} \frac{m_{t+s}^n}{m_{t+s}^{n'}} = 0$. Since $m_{t+1}^{n'} < \infty$, it must be that m_{t+1}^n tends to zero. This cannot occur in equilibrium, as per Proposition 2 and illustrated by Figure 2. Therefore, it cannot be that two coins with different coin growth rates are both valued in equilibrium. Hence, the refinement of Assumption 2 has no bite and one can again construct many possible equilibria.

7 Extensions

In this section, I present two extensions to the main analysis. First, I model blockchain transaction fees which are endogenous to blockchain congestion. I show that the results are unchanged. Second, I describe the effect of blockchain applications, which ensure a strictly positive value to blockchain-native coins even if they are not used as medium of exchange, on currency competition.

network as of December 2023 is given by 6.25 Bitcoins. The difficulty of the puzzles that miners solve using brute computational force is rescaled every 2,016 such that the rate at which new blocks are added to the blockchain stays (roughly) constant at ten minutes per block. Hence, if very few miners participate in the competition for block rewards, then issuing 6.25 Bitcoins approximately every ten minutes requires little computing power and thus incurs very low real costs. In principle, it is even feasible to operate a blockchain on a single computer. However, operating blockchains *securely* is costly because the participants of the network, who must incur real economic costs in order to fence off potential attackers, need to be compensated accordingly. It is the security maintenance process of blockchains that is costly, not the issuance of new coins itself.

7.1 Transaction fees

The main analysis abstracted away from transaction fees. In reality, block rewards consist both of newly issued coins as well as transaction fees, which are a function of blockchain capacity utilization (Lehar and Parlour, 2020).

The model is robust to introducing transaction fees which are endogenous and modelled as follows. First, the level of transaction fees is given by $f_t^n = f(h_t^n)$, where $f : [0,1] \to \mathbb{R}_0^+$. I assume that transaction fees are weakly increasing in the degree of congestion: $f'(h) \geq 0$ for all $h \in [0,1]$. Second, transactions fees are proportional to the transfer. The fees paid by buyer j using coin n are therefore given by $f_t^n D_{j,t}$. Third, transaction fees are paid immediately in the same coin that is transferred to the seller. The cash constraint thus reads $D_{j,t}(1 + f_t^n) \leq M_{j,t}^n$.

The transaction verification probability continues to capture all other nuisances arising due to blockchain congestion. The value function at the time-t DM in the augmented model with transaction fees is then given by

$$V_{j,t}^n\left(M_{j,t}^n\right) = \max_{(q_{j,t},D_{j,t})\in\mathbb{R}_0^+\times\mathbb{R}} \alpha_t^n\left[u(q_{j,t}) + \beta W_{j,t+1}\left(M_{j,t}^n - D_{j,t}(1+f_t^n)\right)\right] + (1-\alpha_t^n)\cdot\beta W_{j,t+1}\left(M_{j,t}^n\right)$$

$$\text{s.t.} \quad D_{j,t}(1+f_t^n) \leq M_{j,t}^n$$

$$q_{j,t} \leq \beta\phi_{t+1}^n D_{j,t}$$

Otherwise, the set-up is unchanged. In Appendix G.1, I solve for optimal consumption in the DM as a function of transaction fees and real coin balances, as well as for optimal coin demand in the CM, all in perfect analogy to the main analysis. The previous results remain intact:

Proposition 8. *Consider $n, n' \in \mathcal{M}$. Then $\pi_{t+1}^n > \pi_{t+1}^{n'}$ if and only if $\alpha_t^n > \alpha_t^{n'}$ (Proposition 1). Furthermore, the following are equivalent: $m_t^n < m_t^{n'}$, $\pi_{t+1}^n > \pi_{t+1}^{n'}$, and $\mu^n > \mu^{n'}$ (Proposition 2).*

The proof is provided in Appendices G.2 and G.3. In the main analysis, holders of coins with relatively lower transaction verification probabilities due to blockchain congestion had to be compensated with lower inflation rates. Otherwise no buyer would hold such high-congestion coins. This continues to be true with transaction fees, which further increase the relative cost of using coins with high congestion blockchains. The negative relationship between congestion and inflation

rates thus continues to hold.

From here the analysis follows in perfect analogy, with adjustments needed to incorporate transaction fees into the definition of $\underline{\mu}$. Entrepreneurs again face strict incentives to undercut other entrepreneurs in order to boost money demand. This increase in demand not only increases the real value of any newly issued coins but also the level of both nominal and real transaction fees.

7.2 Blockchain applications ensure currency competition

Blockchains not only provide coins which can in principle be used as medium of exchange but also offer other use cases which generate real economic value. For example, blockchains are used as decentralized registers of ownership over digital assets, commonly referred to as non-fungible tokens (NFTs). Since purchasing assets registered on a blockchain requires a transfer in the blockchain-native coin, this coin is then backed by the assets' real income stream.

Indeed, consider some finite time τ at which an owner sells their asset registered on the blockchain and the market value of all blockchain-native coins lies below the real asset value. Such a scenario presents a clear arbitrage opportunity and cannot occur in equilibrium. Instead, potential purchasers of the asset bid up the price of the blockchain-native coin until the market value corresponds to a level bound from below by the real asset value. From here it follows that $\phi_\tau^n > 0$. It then cannot be that $\phi_t^n = 0$ for any $\tau \geq t \geq 0$ as purchasing all blockchain-native coins at a zero price generates an infinite return. Then as long as assets are registered on the blockchain, we have $\phi_t^n > 0$ for all t.

Blockchain applications have two immediate implications. First, let $\tilde{\mathcal{N}} \subset \mathcal{N}$ denote the non-empty set of blockchains with applications such that $\phi_t^n > 0$ for all $n \in \tilde{\mathcal{N}}$. Then $\tilde{\mathcal{N}} \subseteq \mathcal{M}$, and hence the set $\mathcal{M}$ must be non-empty. As a consequence, blockchain applications relax the need to refine the equilibrium with regards to which coins are valued.

Second, the result of Proposition 2 holds (in slightly altered form) even in the absence of blockchain security constraints. Set $A = 0$. Let $\underline{m}^n \in \mathbb{R}^+$ denote the lower bound for real coin balances of blockchain $n \in \tilde{\mathcal{N}}$, assumed to be constant for simplicity.

Proposition 9. *Consider two coins $n \in \mathcal{M}$, $n \notin \tilde{\mathcal{N}}$, and $n' \in \tilde{\mathcal{N}}$. Then $m_t^n < m_t^{n'}$ if $\mu^n > \mu^{n'}$.*

See Appendix G.4 for the proof. The blockchain security constraint ensured that the path for real coin balances cannot lead to zero, and hence low growth coins experienced low inflation rates.

A similar logic applies with blockchain applications. Not only must coins native to blockchains with additional applications be valued in equilibrium, they also must have greater market value than their competitor coins if the competitor coin grows at a higher rate. It is in this sense that blockchain applications ensure currency competition, which is facilitated by blockchain congestion in the first place.

8 Conclusion

This paper argues that the apparent drawbacks of blockchain-operated currencies, namely capacity constraints and security costs, emerge as distinctive features when viewed within the context of currency competition. Issuers of cryptocurrencies face strict incentives to undercut other cryptocurrencies' money growth rates in order to boost demand. This leads to low-inflation outcomes but comes at the cost of unrealized gains from trade—even in the absence of any network effects—as well as inefficiently high levels of inflation in equilibrium. The paper thus highlights a continuing role for public, centralized money.

References

Benigno, P., L. M. Schilling, and H. Uhlig (2022): "Cryptocurrencies, currency competition, and the impossible trinity," *Journal of international economics*, 136, 103601.

Bertucci, L. (2020): "Incentives on the lightning network: A blockchain-based payment network," in *Proceedings of Paris December 2020 Finance Meeting EUROFIDAI-ESSEC*.

Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta (2019): "The blockchain folk theorem," *The Review of Financial Studies*, 32, 1662–1715.

Biais, B., C. Bisiere, M. Bouvard, C. Casamatta, and A. J. Menkveld (2023): "Equilibrium bitcoin pricing," *The Journal of Finance*, 78, 967–1014.

Budish, E. (2023): "Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains," *University of Chicago Working Paper*.

Cong, L. W., X. Hui, C. Tucker, and L. Zhou (2023): "Scaling smart contracts via layer-2 technologies: Some empirical evidence," *Management Science*, 69, 7306–7316.

Cong, L. W. and S. Mayer (2022): "The Coming Battle of Digital Currencies," *Available at SSRN 3992815*.

Divakaruni, A. and P. Zimmerman (2023): "The lightning network: Turning bitcoin into money," *Finance Research Letters*, 52, 103480.

Fernández-Villaverde, J. and D. Sanches (2019): "Can Currency Competition Work?" *Journal of Monetary Economics*, 106, 1–15.

Garratt, R. and M. R. van Oordt (2023): "Why fixed costs matter for proof-of-work based cryptocurrencies," *Management science (forthcoming)*.

Guasoni, P., G. Huberman, and C. Shikhelman (2023a): "Lightning network economics: Channels," *Management Science*.

——— (2023b): "Lightning network economics: Topology," *Available at SSRN 4439190*.

Guennewig, M. (2024): "Currency Competition with Firms," *Available at SSRN 3624671*.

Hinzen, F. J., K. John, and F. Saleh (2022): "Bitcoin's limited adoption problem," *Journal of Financial Economics*, 144, 347–369.

Huberman, G., J. D. Leshno, and C. Moallemi (2021): "Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System," *The Review of Economic Studies*, 88, 3011–3040.

John, K., M. O'Hara, and F. Saleh (2021): "Bitcoin and Beyond," *Annual Review of Financial Economics*, 14.

John, K., T. J. Rivera, and F. Saleh (2022): "Economic implications of scaling blockchains: Why the consensus protocol matters," *Available at SSRN 3750467*.

Kareken, J. and N. Wallace (1981): "On the Indeterminacy of Equilibrium Exchange Rates," *The Quarterly Journal of Economics*, 96, 207–222.

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

Lehar, A. and C. A. Parlour (2020): "Miner collusion and the bitcoin protocol," *Available at SSRN 3559894*.

Manuelli, R. E. and J. Peck (1990): "Exchange rate volatility in an equilibrium asset pricing model," *International Economic Review*, 559–574.

Obstfeld, M. and K. Rogoff (1983): "Speculative Hyperinflations in Maximizing Models: Can We Rule Them Out?" *Journal of Political Economy*, 91, 675–687.

Pagnotta, E. S. (2022): "Decentralizing money: Bitcoin prices and blockchain security," *The Review of Financial Studies*, 35, 866–907.

Prat, J. and B. Walter (2021): "An Equilibrium Model of the Market for Bitcoin Mining," *Journal of Political Economy*, 129, 2415–2452.

Saleh, F. (2021): "Blockchain without waste: Proof-of-stake," *The Review of financial studies*, 34, 1156–1190.

Schilling, L. and H. Uhlig (2019): "Some Simple Bitcoin Economics," *Journal of Monetary Economics*, 106, 16–26.

Williamson, S. D. (2012): "Liquidity, monetary policy, and the financial crisis: A new monetarist approach," *American Economic Review*, 102, 2570–2605.

Wright, R., P. Kircher, B. Julien, and V. Guerrieri (2021): "Directed search and competitive search equilibrium: A guided tour," *Journal of Economic Literature*, 59, 90–148.

Appendices

A Proof of Proposition 2

I prove the proposition with the help of two lemmata. Suppose Condition 1 is satisfied, implying that $u'(q) \cdot q$ is weakly increasing for all $q \in [0, q^*]$.

Lemma 4. *Consider $n, n' \in \mathcal{M}$. If $\pi_{t+1}^n > \pi_{t+1}^{n'}$, then $m_t^n < m_t^{n'}$.*

Proof. Suppose $\pi_{t+1}^n > \pi_{t+1}^{n'}$. Note that this implies that the cash constraint is binding for coin n. Proposition 1 implies that $\alpha_t^n > \alpha_t^{n'}$ and $\tilde{m}_{j,t}^n < \tilde{m}_{j,t}^{n'}$. Equation (1) then necessitates $h_t^n < h_t^{n'}$, with $h_t^{n'} > \eta$. Equation (1) further implies that $h_t^n \alpha_t^n = \min\{h_t^n, \eta\}$ and $h_t^{n'} \alpha_t^{n'} = \eta$. Using Equation (3), m_t^n is given by

$$m_t^n \;=\; h_t^n m_{j,t}^n \;=\; \min\{h_t^n, \eta\} \cdot u'(\tilde{m}_{j,t}^n) \cdot \tilde{m}_{j,t}^n \;+\; (1 - \alpha_t^n) \cdot h_t^n \tilde{m}_{j,t}^n$$

If the cash constraint is also binding for coin n', then $m_t^{n'}$ is given by

$$m_t^{n'} \;=\; h_t^{n'} m_{j,t}^{n'} \;=\; \eta \cdot u'(\tilde{m}_{j,t}^{n'}) \cdot \tilde{m}_{j,t}^{n'} \;+\; (1 - \alpha_t^{n'}) \cdot h_t^{n'} \tilde{m}_{j,t}^{n'} \;>\; m_t^n$$

If the cash constraint is not binding for coin n', then $\phi_t^{n'} = \beta \phi_{t+1}^{n'}$ and hence $m_{j,t}^{n'} = \tilde{m}_{j,t}^{n'} \geq q^*$. Then

$$\begin{aligned}
m_{j,t}^{n'} \;&=\; \alpha_t^{n'} \cdot m_{j,t}^{n'} \;+\; (1 - \alpha_t^{n'}) \cdot m_{j,t}^{n'} \\
&\geq\; \alpha_t^{n'} \cdot q^* \;+\; (1 - \alpha_t^{n'}) \cdot m_{j,t}^{n'} \\
&=\; \alpha_t^{n'} \cdot u'(q^*) \cdot q^* \;+\; (1 - \alpha_t^{n'}) \cdot \tilde{m}_{j,t}^{n'} \\
&\geq\; \alpha_t^{n'} \cdot u'\left(\tilde{m}_{j,t}^n\right) \cdot \tilde{m}_{j,t}^n \;+\; (1 - \alpha_t^{n'}) \cdot \tilde{m}_{j,t}^{n'}
\end{aligned}$$

Multiplying both sides by $h_t^{n'}$ reveals

$$\begin{aligned}
m_t^{n'} \;&\geq\; \min\{h_t^{n'}, \eta\} \cdot u'\left(\tilde{m}_{j,t}^n\right) \cdot \tilde{m}_{j,t}^n \;+\; (1 - \alpha_t^{n'}) \cdot h_t^{n'} \cdot \tilde{m}_{j,t}^{n'} \\
&>\; \min\{h_t^n, \eta\} \cdot u'\left(\tilde{m}_{j,t}^n\right) \cdot \tilde{m}_{j,t}^n \;+\; (1 - \alpha_t^n) \cdot h_t^n \cdot m_{j,t}^n \\
&=\; m_t^n
\end{aligned}$$

The claim follows. □

Lemma 5. *Consider $n, n' \in \mathcal{M}$. If $\mu^n > \mu^{n'}$, then $\pi_{t+1}^n \geq \pi_{t+1}^{n'}$ for all $t \geq 0$.*

Proof. The proof is by contradiction. Let $\mu^n > \mu^{n'}$. Suppose $\pi_{t+1}^n < \pi_{t+1}^{n'}$ for at least one $t \geq 0$. By

definition, aggregate real coin balances in coin n evolve according to

$$m_{t+1}^n \;=\; \frac{1+\mu^n}{1+\pi_{t+1}^n}\cdot m_t^n$$

and hence

$$\frac{m_{t+1}^n}{m_{t+1}^{n'}} \;=\; \frac{1+\mu^n}{1+\mu^{n'}}\cdot\frac{1+\pi_{t+1}^{n'}}{1+\pi_{t+1}^n}\cdot\frac{m_t^n}{m_t^{n'}}$$

By Lemma 4, if $\pi_{t+1}^n < \pi_{t+1}^{n'}$, then $m_t^n > m_t^{n'}$. Since $\mu^n > \mu^{n'}$ and $\pi_{t+1}^n < \pi_{t+1}^{n'}$, it must be that $\frac{m_{t+1}^n}{m_{t+1}^{n'}} > \frac{m_t^n}{m_t^{n'}}$, and thus $m_{t+1}^n > m_{t+1}^{n'}$. By Lemma 4, this necessitates $\pi_{t+2}^n \leq \pi_{t+2}^{n'}$ as otherwise $m_{t+1}^n < m_{t+1}^{n'}$. Following the same steps shows that $\frac{m_{t+2}^n}{m_{t+2}^{n'}} > \frac{m_{t+1}^n}{m_{t+1}^{n'}}$ and thus $m_{t+2}^n > m_{t+2}^{n'}$, implying that $\pi_{t+3}^n \leq \pi_{t+3}^{n'}$. From here it is clear that $m_{t+s}^n > m_{t+s}^{n'}$ and $\pi_{t+s+1}^n \leq \pi_{t+s+1}^{n'}$ for all $s \geq 1$. It follows that

$$\lim_{s\to\infty}\frac{m_{t+s}^n}{m_{t+s}^{n'}} \;=\; \lim_{s\to\infty}\left(\frac{1+\mu^n}{1+\mu^{n'}}\right)^s\cdot\prod_{k=1}^{s}\frac{1+\pi_{t+k}^{n'}}{1+\pi_{t+k}^n}\cdot\frac{m_t^n}{m_t^{n'}} \;\to\; \infty$$

Since $m_t^n < \infty$ for all $t \geq 0$, it must be that $m_{t+s}^{n'} \searrow 0$ as $s \to \infty$. But then $\frac{\mu^{n'}}{1+\mu^{n'}} m_\tau^{n'} < A$ at some finite τ for all $\mu^{n'} < \infty$, at which point $\phi_\tau^{n'} = 0$. This in turn implies that $\phi_{\tau-1}^{n'} = 0$ by Equation (3), and hence $\phi_t^{n'} = 0$ for all $t \geq 0$. This is a contradiction to $n' \in \mathcal{M}$, and the claim follows. □

To complete the proof, consider $n, n' \in \mathcal{M}$ and let $\mu^n > \mu^{n'}$. Suppose $\pi_{t+1}^n > \pi_{t+1}^{n'}$ for all $t \geq 0$. The claim then trivially follows from Lemma 4. Suppose $\pi_{t+1}^n = \pi_{t+1}^{n'}$ for at least one $t \geq 0$. If $m_t^n < m_t^{n'}$ for all these $t \geq 0$, the claim again trivially follows. Hence suppose $\pi_{t+1}^n = \pi_{t+1}^{n'}$ and $m_t^n \geq m_t^{n'}$ for at least one $t \geq 0$. Since

$$\frac{m_{t+1}^n}{m_{t+1}^{n'}} \;=\; \frac{1+\mu^n}{1+\mu^{n'}}\cdot\frac{1+\pi_{t+1}^{n'}}{1+\pi_{t+1}^n}\cdot\frac{m_t^n}{m_t^{n'}}$$

it must be that $m_{t+1}^n > m_{t+1}^{n'}$. This requires $\pi_{t+2}^n \leq \pi_{t+2}^{n'}$, and hence $\frac{m_{t+2}^n}{m_{t+2}^{n'}} > \frac{m_{t+1}^n}{m_{t+1}^{n'}}$ as well as $m_{t+2}^n > m_{t+2}^{n'}$. This again requires $\pi_{t+3}^n \leq \pi_{t+3}^{n'}$. Continuing this logic, it follows that

$$\lim_{s\to\infty}\frac{m_{t+s}^n}{m_{t+s}^{n'}} \;=\; \lim_{s\to\infty}\left(\frac{1+\mu^n}{1+\mu^{n'}}\right)^s\cdot\prod_{k=1}^{s}\frac{1+\pi_{t+k}^{n'}}{1+\pi_{t+k}^n}\cdot\frac{m_t^n}{m_t^{n'}} \;\to\; \infty$$

yielding the same contradiction to $n' \in \mathcal{M}$ as in the proof of Lemma 4. The claim follows.

B Proof of Lemma 2

Proof. Consider monetary policy $\boldsymbol{\mu}$ such that $\mathcal{M} = \mathcal{N}$ and $h_t^n \leq \eta$ for all $n \in \mathcal{N}$. Consider further $m_{j,t}^n = m_j$, $\tilde{m}_{j,t}^n = \tilde{m}_j$, and $h_t^n = 1/N$ satisfying

$$\frac{\mu}{1+\mu} \cdot \frac{m_j}{N} \;\geq\; A$$

for all $n \in \mathcal{N}$ and $t \geq 0$. Consider a deviation in monetary policy $\mu^n = \mu - \varepsilon < \mu$ for some $n \in \mathcal{M}$, and suppose

$$\lim_{\varepsilon \searrow 0} m_{j,t}^n(\mu^n, \boldsymbol{\mu}^{-1}) \;=\; m_{j,t}^n(\boldsymbol{\mu}) \;=\; m_j \qquad \text{and} \qquad \lim_{\varepsilon \searrow 0} \tilde{m}_{j,t}^n(\mu^n, \boldsymbol{\mu}^{-1}) \;=\; \tilde{m}_{j,t}^n(\boldsymbol{\mu}) \;=\; \tilde{m}_j$$

Since

$$m_{j,t}^n \;=\; \alpha_t^n \cdot u'\left(\tilde{m}_{j,t}^n\right) \cdot \tilde{m}_{j,t}^n + (1 - \alpha_t^n) \cdot \tilde{m}_{j,t}^n$$

it must be that α_t^n tends to one, and thus h_t^n tends to η. Suppose that consumer j real coin balances remain unchanged for all the coins $n' \neq n$ that continue to be valued. The respective security blockchain constraints continue to be satisfied if there exists a number of coins $\hat{N} \in \{1, ..., N-1\}$ satisfying

$$\eta \;\geq\; \frac{1-\eta}{\hat{N}} \;\geq\; \frac{1}{N}$$

The first inequality ensures that the $\hat{N}$ coins which remain valued can cover the $1 - \eta$ mass of buyers not using coin n without becoming congested. Rearranging yields $\eta \geq \frac{1}{\hat{N}+1}$. The second inequality ensures that the mass of buyers $1 - \eta$ is sufficiently high such that at least $\hat{N}$ coins have a weakly larger buyer base after the deviation, ensuring that the blockchain security constraint remains satisfied. Rearranging yields $\eta \leq \frac{N-\hat{N}}{N}$. Combine to read

$$\frac{1}{\hat{N}+1} \;\leq\; \eta \;\leq\; \frac{N-\hat{N}}{N}$$

These inequalities can jointly be satisfied for a sufficiently large N. Since N is arbitrarily large, the deviation is consistent with equilibrium conditions, and the claim follows. □

C Proof of Proposition 3

Proof. Consider the symmetric strategies $\boldsymbol{\mu}$ with $\mu^n = \mu > \mu(1)$ for all $n \in \mathcal{N}$. Suppose $\mathcal{M} \subset N$. Any $n \notin \mathcal{M}$ achieves a zero payoff. Consider a deviation $\mu^n = \mu(1)$ for some $n \notin \mathcal{M}$. By Assumption 1, such a monetary policy is consistent with a monetary equilibrium. By Assumption 2 and since $\mu^{n'} > \mu^n = \mu(1)$ for all $n' \in \mathcal{N}$, $n' \neq n$, it must be that $m_t^n > 0$ for all $t \geq 0$. Entrepreneur n achieves a strictly positive payoff and thus faces a profitable deviation to set $\mu^n = \mu(1)$.

Next, suppose $\mathcal{M} = \mathcal{N}$. Since $(N-1) \cdot \eta > 1$, we have $h_t^n < \eta$ for at least two n. Consider one of these n, and consider a marginal deviation $\mu^n = \mu - \varepsilon$, with $\varepsilon \searrow 0$. By Assumption 3, we have $\lim_{\varepsilon \searrow 0} m_{j,t}^n(\mu^n, \boldsymbol{\mu}^{-n}) = m_{j,t}^n(\boldsymbol{\mu})$ as well as $\lim_{\varepsilon \searrow 0} \tilde{m}_{j,t}^n(\mu^n, \boldsymbol{\mu}^{-n}) = \tilde{m}_{j,t}^n(\boldsymbol{\mu})$. Since

$$m_{j,t}^n(\boldsymbol{\mu}) \;=\; \alpha_t^n \cdot u'\left(\tilde{m}_{j,t}^n(\boldsymbol{\mu})\right) \cdot \tilde{m}_{j,t}^n(\boldsymbol{\mu}) + (1 - \alpha_t^n) \cdot \tilde{m}_{j,t}^n(\boldsymbol{\mu})$$

it must be that α_t^n tends to one which requires that h_t^n tends to η.

$$\lim_{\varepsilon \searrow 0} x_t^n \;=\; \frac{\mu}{1+\mu} \cdot \eta \cdot m_{j,t}^n(\boldsymbol{\mu}) \;>\; \frac{\mu}{1+\mu} \cdot h_t^n \cdot m_{j,t}^n(\boldsymbol{\mu})$$

By Lemma 2, the above is consistent with the equilibrium conditions. Entrepreneur n thus faces a profitable deviation, and the claim follows. □

D Proof of Proposition 4

The proof is by contradiction. Suppose otherwise, and $h_t^n \leq \eta$ for all $n \in \mathcal{M}$ for at least one $t \geq 0$. Then $\alpha_t^n = \alpha_{t+1}^{n'}$ for all $n, n' \in \mathcal{M}$ for all $n, n' \in \mathcal{M}$, and hence $\pi_{t+1}^n = \pi_{t+1}^{n'}$ for all $n, n' \in \mathcal{M}$ by Proposition 1. Furthermore, since $\sum_{n \in \mathcal{M}} h_t^n = 1$ for all $t \geq 0$, it must be that $\eta \cdot |\mathcal{M}| \geq 1$.

Consider the first time period $t \geq 0$ in which $h_t^n \leq \eta$ for all $n \in \mathcal{M}$. Suppose $m_t^n = m_t^{n'}$ for all $n, n' \in \mathcal{M}$. Since $\pi_{t+1}^n = \pi_{t+1}^{n'}$ and $\mu^n = \mu^{n'}$ for all $n, n' \in \mathcal{M}$, we have $m_{t+1}^n = m_{t+1}^{n'}$ which by Lemma 4 requires $\pi_{t+2}^n = \pi_{t+2}^{n'}$. It then follows that $m_{t+2}^n = m_{t+2}^{n'}$ and $\pi_{t+3}^n = \pi_{t+3}^{n'}$, and hence $m_{t+s}^n = m_{t+s}^{n'}$ and $\pi_{t+s+1}^n = \pi_{t+s+1}^{n'}$ for all $s \geq 0$. Since $h_t^n = h_t^{n'} \leq \eta$, it must be that $h_{t+s}^n = h_{t+s}^{n'} \leq \eta$ for all $s \geq 0$.

Next, suppose $m_t^n \neq m_t^{n'}$ for all $n, n' \in \mathcal{M}$. Consider coin n with $m_t^n \leq m_t^{n'}$ for all $n' \in \mathcal{M}$,

with the inequality strict for at least one n'. If $m_t^n = m_t^{n'}$ for some $n' \in \mathcal{M}$, then by the previous logic it must be that $m_{t+s}^n = m_{t+s}^{n'}$ and $\pi_{t+s+1}^n = \pi_{t+s+1}^{n'}$ as well as $h_{t+s}^n = h_{t+s}^{n'}$ for all $s \geq 0$. If $m_t^n < m_t^{n'}$ for some $n' \in \mathcal{M}$, then $h_t^n < h_t^{n'}$. With $\pi_{t+1}^n = \pi_{t+1}^{n'}$ and $\mu^n = \mu^{n'}$, it must be that $m_{t+1}^n < m_{t+1}^{n'}$ as well as $\pi_{t+2}^n \geq \pi_{t+2}^{n'}$. This implies $h_{t+1}^n < h_{t+1}^{n'}$. Repeating the same exercise, it must be that $m_{t+2}^n < m_{t+2}^{n'}$, $\pi_{t+3}^n \geq \pi_{t+3}^{n'}$ and $h_{t+2}^n < h_{t+2}^{n'}$. From here it follows that $m_{t+s}^n < m_{t+s}^{n'}$, $\pi_{t+s+1}^n \geq \pi_{t+s+1}^{n'}$ and $h_{t+s}^n < h_{t+s}^{n'}$ for all $s \geq 0$. Since $\sum_{n \in \mathcal{M}} h_s^n = 1$ for all $t \geq 0$ and $\eta \cdot |\mathcal{M}| \geq 1$, it must be that $h_{t+s}^n < \eta$ for all $s \geq 0$.

Note that money balances are unbounded if $\pi_{t+1}^n < \mu^n$ for all $t \geq 0$, and hence $\pi_{t+1}^n \geq \mu^n$ for all $n \in \mathcal{M}$ for at least one $t \geq 0$.

I will now show that the blockchain security constraint (Equation 2) is violated for coin n with $\mu^n \leq \underline{\mu}(1) < \underline{\mu}(\eta)$ if $h_{t+s}^n \leq \eta$ and $\pi_{t+s+1}^n \geq \mu^n$ for some $s \geq 0$. Consider Equations (2) and (3) for uncongested blockchains:

$$\frac{\mu^n}{1+\mu^n} \cdot h_{t+s}^n \cdot (1 + \pi_{t+s+1}^n) \cdot \frac{\tilde{m}_{j,t+s}^n}{\beta} \;\geq\; A$$

and $1 + \pi_{t+s+1}^n = \beta u'(\tilde{m}_{j,t+s}^n)$. Substitute the latter into the former to find

$$\frac{\mu^n}{1+\mu^n} \cdot h_{t+s}^n \cdot u'\left(\tilde{m}_{j,t+s}^n\right) \cdot \tilde{m}_{j,t+s}^n \;\geq\; A \tag{ID.1}$$

Clearly, the LHS of (ID.1) is strictly increasing in $h_{t+s}^n \leq \eta$. Note that $\tilde{m}_{j,t+s}^n$ is strictly decreasing in π_{t+s+1}^n. With Condition 1, the LHS of (ID.1) is then strictly decreasing in π_{t+s+1}^n. Recall the definition of $\underline{\mu}(\eta)$ as the lowest $\mu \in \mathbb{R}^+$ that satisfies (ID.1) with equality for $\pi_{t+s+1}^n = \mu^n$ and $h_{t+s}^n = \eta$.[17] By definition, (ID.1) cannot be satisfied if $\mu^n < \underline{\mu}(\eta)$, $\pi_{t+s+1}^n = \mu^n$ and $h_{t+s}^n = \eta$. Hence it cannot be satisfied if $\mu^n < \underline{\mu}(\eta)$, $\pi_{t+s+1}^n \geq \mu^n$ and $h_{t+s}^n \leq \eta$.

Since $h_t^n \leq \eta$ for all $n \in \mathcal{M}$ for at least one $t \geq 0$ implies that $h_t^n \leq \eta$ for at least one $n \in \mathcal{M}$ for all $t \geq 0$, and since $\mu^n \leq \underline{\mu}(1) < \underline{\mu}(\eta)$ by Proposition 3, we have a contradiction, as coin n cannot be contained in the set $\mathcal{M}$. The claim follows.

[17] The value $\underline{\mu}(\eta)$ is of course equivalent, regardless whether it is defined based on Equation (6) or based on Equation (ID.1) in its binding form with $h_{t+s}^n = \eta$ and $\pi_{t+s+1}^n = \mu^n$.

E Proof of Lemma 3

Let $G : (\mathbb{R}^+)^3 \to \mathbb{R}$ be a continuously differentiable function given by

$$G(x_1, x_2, y) \;=\; -(1+y) \;+\; \beta \frac{x_1}{x_2} \cdot u'\left(\frac{\beta A}{y x_2}\right) + \beta\left(1 - \frac{x_1}{x_2}\right)$$

with

$$G_y(x_1, x_2, y) \;=\; -1 \;-\; \frac{1}{y} \cdot \beta \frac{x_1}{x_2} \cdot u''\left(\frac{\beta A}{y x_2}\right) \cdot \frac{\beta A}{y x_2}$$

and

$$G_{x_2}(x_1, x_2, y) \;=\; \beta \frac{x_1}{(x_2)^2}\left[1 - u'\left(\frac{\beta A}{y x_2}\right) - u''\left(\frac{\beta A}{y x_2}\right) \cdot \frac{\beta A}{y x_2}\right]$$

Fix a point (η_0, h_0, μ_0) such that $G(\eta_0, h_0, \mu_0) = 0$ as well as $G_y(\eta_0, h_0, \mu_0) > 0$. Then, by the implicit function theorem, there exists an open set $S \subset (\mathbb{R}^+)^2$ containing (η_0, h_0) such that there exists a continuously differentiable function $g : S \to \mathbb{R}_0^+$ such that

i. $g(\eta_0, h_0) = \mu_0$ and $G\left(x_1, x_2, g(x_1, x_2)\right) = 0$ for all $(x_1, x_2) \in S$.

ii. the partial derivative of g in S for x_i, $i \in \{1, 2\}$, reads

$$g_{x_i}(x_1, x_2) \;=\; -\frac{G_{x_i}(x_1, x_2, g(x_1, x_2))}{G_y(x_1, x_2, g(x_1, x_2))}$$

Consider $(x_1, x_2) = (1, 1)$ and suppose $1 > u'\left(\frac{\beta A}{\tilde{\mu}}\right) + u''\left(\frac{\beta A}{\tilde{\mu}}\right) \cdot \frac{\beta A}{\tilde{\mu}}$. It immediately follows that $G_{x_2}(1, 1, \tilde{\mu}) > 0$. Since $G(1, 1, \tilde{\mu}) = 0$ by definition, note that $G_y(1, 1, \tilde{\mu}) > 0$ as

$$-\tilde{\mu} - \beta \cdot u''\left(\frac{\beta A}{\tilde{\mu}}\right) \cdot \frac{\beta A}{\tilde{\mu}} \;=\; 1 - \beta \cdot u'\left(\frac{\beta A}{\tilde{\mu}}\right) - \beta \cdot u''\left(\frac{\beta A}{\tilde{\mu}}\right) \cdot \frac{\beta A}{\tilde{\mu}} \;>\; 0$$

The implicit function theorem therefore applies at $(x_1, x_2) = (1, 1)$.

Recall the definition of $\underline{\mu}$ as function assigning to each $h \in [\eta, 1]$ the lowest level of μ that satisfies Equation (6) for a given level of η. By Assumption 1, there exists at least one $\mu \in \mathbb{R}^+$ for a given level of $\eta \in (0, 1]$ for all $h \in [\eta, 1]$ such that Equation (6) is satisfied; by the assumptions on u, there can be at most two. If there are two, it must be that $G_y(\eta, h, \mu) > 0$ at the lowest level of $\mu \in \mathbb{R}^+$ that satisfies Equation (6). It then follows that the function $\underline{\mu}$ assigns the same value to h

for a given level of η as g assigns to $(x_1, x_2) = (\eta, h)$ whenever g exists with $G_y(\eta, h, g(\eta, h)) > 0$. Hence $g(1,1) = \tilde{\mu}$.

Condition 2 is satisfied if $\underline{\mu}$ is a decreasing function in h. Consequentially, it is satisfied if g exists and $g_{x_2}(x_1, x_2) < 0$ for $x_1 = \eta \in (0, 1]$ and for all $x_2 \in [\eta, 1]$. Since g is continuously differentiable in S, so is $G_{x_2}(x_1, x_2, g(x_1, x_2))$. It then follows that there exists a neighborhood around $(x_1, x_2) = (1, 1)$ containing the set of points $\{\eta, h\}_{h\in[\eta,1]}$, with $\eta < 1$, such that $G_{x_2}(\eta, h, g(\eta, h)) > 0$ for all $h \in [\eta, 1]$. Hence, there exists an $\underline{\eta} \in (0, 1)$ such that $\underline{\mu}(1) < \underline{\mu}(h)$ for all $h \in [\eta, 1]$ if $\eta \geq \underline{\eta}$.

F Proof of Proposition 7

Proof. Entrepreneur n's problem (Equation 7) reads

$$\underset{\mu^n \in \mathbb{R}_0^+}{max} \quad \sum_{t\geq 0} \frac{\mu^n}{1+\mu^n} \cdot m_t^n$$

which can be re-stated as

$$\underset{\mu^n \in \mathbb{R}_0^+}{max} \quad \frac{\mu^n}{1+\mu^n} \cdot \phi_0^n \cdot M_0^n \; + \sum_{t\geq 1} \frac{\mu^n}{1+\mu^n} \cdot m_t^n$$

Since $M_0^n = (1+\mu^n)M_{-1}$, we have

$$\underset{\mu^n \in \mathbb{R}_0^+}{max} \quad \mu^n \cdot \phi_0^n \cdot M_{-1} \; + \sum_{t\geq 1} \frac{\mu^n}{1+\mu^n} \cdot m_t^n$$

Then, for any $\phi_0^n > 0$, it cannot be optimal to set $\mu^n < \infty$; the problem does not have a solution. The claim follows. □

G Appendix: Extensions

G.1 Appendix: Transaction fees

The value function at the time-t CM when holding a particular coin n is unchanged:

$$W_{j,t}^n(M) \;=\; \max_{M_{j,t}^n \in \mathbb{R}_0^+} \phi_t^{n'} M - \phi_t^n M_{j,t}^n + V_{j,t}^n\left(M_{j,t}^n\right)$$

whereas the value function of the time-t DM now reads

$$V_{j,t}^n\left(M_{j,t}^n\right) \;=\; \max_{(q_{j,t},D_{j,t})\in\mathbb{R}_0^+\times\mathbb{R}} \alpha_t^n\left[u(q_{j,t}) + \beta W_{j,t+1}\left(M_{j,t}^n - D_{j,t}(1+f_t^n)\right)\right] + (1-\alpha_t^n)\cdot\beta W_{j,t+1}\left(M_{j,t}^n\right)$$

$$\text{s.t.} \quad D_{j,t}(1+f_t^n) \;\leq\; M_{j,t}^n$$

$$q_{j,t} \;\leq\; \beta\phi_{t+1}^n D_{j,t}$$

As before, the optimal transfer is given by the quantity produced: $q_{j,t} = \beta\phi_{t+1}^n D_{j,t}$. Making use of quasi-linearity, the value function simplifies to

$$V_{j,t}^n\left(M_{j,t}^n\right) \;=\; \max_{q_{j,t}\in\mathbb{R}_0^+} \alpha_t^n\left[u(q_{j,t}) - (1+f_t^n)q_{j,t}\right] + \beta\left[\phi_{t+1}^n M_{j,t}^n + W_{j,t+1}(0)\right]$$

$$\text{s.t.} \quad (1+f_t^n)q_{j,t} \;\leq\; \beta\phi_{t+1}^n M_{j,t}^n$$

Let $q(f_t^n)$ denote the level of q that satisfies $u'\big(q(f_t^n)\big) = 1 + f_t^n$. Consumption conditional on successful transaction verification is then given

$$q_{j,t} \;=\; \begin{cases} q(f_t^n) & \text{if} \quad (1+f_t^n)\cdot q(f_t^n) \;\leq\; \beta\phi_{t+1}^n M_{j,t}^n \\ \frac{\beta\phi_{t+1}^n M_{j,t}^n}{1+f_t^n} & \text{otherwise} \end{cases}$$

As before, if the cash constraint is not binding, then

$$\phi_t^n \;=\; \beta\phi_{t+1}^n$$

Otherwise, optimal coin demand is characterized by the new first order condition:

$$\phi_t^n \;=\; \alpha_t^n \cdot u'\left(\frac{\beta\phi_{t+1}^n M_{j,t}^n}{1+f_t^n}\right)\cdot\frac{\beta\phi_{t+1}^n}{1+f_t^n} \;+\; (1-\alpha_t^n)\cdot\beta\phi_{t+1}^n$$

The transaction fee essentially scales down the coin balances available to purchase consumption goods. Using this condition, rewrite the value function as before:

$$W_{j,t}^n(M) \;=\; \phi_t^{n'} M \;+\; \alpha_t^n \cdot \psi\left(\frac{\tilde{m}_{j,t}^n}{1+f_t^n}\right) \;+\; \beta W_{j,t+1}(0)$$

where $\psi : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ with $\psi(y) = u(y) - y\cdot u'(y)$ if $0 \le y < q(f_t^n)$, and $\psi(y) = u\big(q(f_t^n)\big) - q(f_t^n)\cdot(1+f_t^n)$ if $y \ge q(f_t^n)$. By the properties of the utility function, note that $\psi(0) = 0$. Also note that $\psi'(y) = -yu''(y) > 0$ if $y \in \big(0, q(f_t^n)\big)$, and $\psi'(y) = 0$ if $y \ge q(f_t^n)$. Indifference between coins again requires

$$\alpha_t^n \cdot \psi\left(\frac{\tilde{m}_{j,t}^n}{1+f_t^n}\right) \;=\; \alpha_t^{n'} \cdot \psi\left(\frac{\tilde{m}_{j,t}^{n'}}{1+f_t^{n'}}\right)$$

I now proceed to prove the claim of Proposition 8.

G.2 Proof of Proposition 8 (equivalent of Proposition 1)

Proof. To show that $\pi_{t+1}^n > \pi_{t+1}^{n'}$ if $\alpha_t^n > \alpha_t^{n'}$, suppose $\alpha_t^n > \alpha_t^{n'}$. This requires $h_t^n < h_t^{n'}$ and thus $f_t^n \le f_t^{n'}$. Equation (4) necessitates that

$$\frac{\tilde{m}_{j,t}^n}{1+f_t^n} \;<\; \frac{\tilde{m}_{j,t}^{n'}}{1+f_t^{n'}}$$

which implies that $0 < \tilde{m}_{j,t}^n < \tilde{m}_{j,t}^{n'}$, with $\tilde{m}_{j,t}^n < q(f_t^n)$. This in turn implies that

$$u'\left(\frac{\tilde{m}_{j,t}^n}{1+f_t^n}\right) \;>\; u'\left(\frac{\tilde{m}_{j,t}^{n'}}{1+f_t^{n'}}\right)$$

if the cash constraint is binding for both coins. Combining first order conditions then reveals that $\pi_{t+1}^n > \pi_{t+1}^{n'}$. If the cash constraint is not binding for coin n', then

$$u'\left(\frac{\tilde{m}_{j,t}^n}{1+f_t^n}\right) \;>\; u'\big(q(f_t^n)\big)$$

It also follows that $\pi_{t+1}^n > \pi_{t+1}^{n'}$.

To show that $\pi_{t+1}^n > \pi_{t+1}^{n'}$ only if $\alpha_t^n > \alpha_t^{n'}$, suppose $\alpha_t^n \leq \alpha_t^{n'}$ and follow the same steps to find that $\pi_{t+1}^n \leq \pi_{t+1}^{n'}$. □

G.3 Proof of Proposition 8 (continued, equivalent of Proposition 2)

Proof. Recall that Proposition 2 was shown using Lemmas 4 and 5. Note that the proof of Lemma 5 applies for any level of $f_t^n \geq 0$. I therefore only need to show that $m_t^n < m_t^{n'}$ if and only if $\pi_{t+1}^n > \pi_{t+1}^{n'}$ (the equivalent of Lemma 4).

First, I show that $m_t^n < m_t^{n'}$ if $\pi_{t+1}^n > \pi_{t+1}^{n'}$. Suppose $\pi_{t+1}^n > \pi_{t+1}^{n'}$. Note that this implies that the cash constraint is binding for coin n. From Appendix G.2 above, we have $\alpha_t^n > \alpha_t^{n'}$, $\frac{\tilde{m}_{j,t}^n}{1+f_t^n} < \frac{\tilde{m}_{j,t}^{n'}}{1+f_t^{n'}}$ and $\tilde{m}_{j,t}^n < \tilde{m}_{j,t}^{n'}$. Equation (1) then necessitates $h_t^n < h_t^{n'}$, with $h_t^{n'} > \eta$. Equation (1) further implies that $h_t^n \alpha_t^n = \min\{h_t^n, \eta\}$ and $h_t^{n'} \alpha_t^{n'} = \eta$.

Using the first order condition, m_t^n is given by

$$m_t^n \;=\; h_t^n m_{j,t}^n \;=\; \min\{h_t^n, \eta\} \cdot u'\left(\frac{\tilde{m}_{j,t}^n}{1+f_t^n}\right) \cdot \frac{\tilde{m}_{j,t}^n}{1+f_t^n} \;+\; (1-\alpha_t^n) \cdot h_t^n \tilde{m}_{j,t}^n$$

If the cash constraint is also binding for coin n', then $m_t^{n'}$ is given by

$$m_t^{n'} \;=\; h_t^{n'} m_{j,t}^{n'} \;=\; \eta \cdot u'\left(\frac{\tilde{m}_{j,t}^{n'}}{1+f_t^{n'}}\right) \cdot \frac{\tilde{m}_{j,t}^{n'}}{1+f_t^{n'}} \;+\; (1-\alpha_t^{n'}) \cdot h_t^{n'} \tilde{m}_{j,t}^{n'}$$

Since $u'(q) \cdot q$ is a weakly increasing function in q, it follows that $m_t^n < m_t^{n'}$.

If the cash constraint is not binding for coin n', then $\frac{m_{j,t}^{n'}}{1+f_t^{n'}} = \frac{\tilde{m}_{j,t}^{n'}}{1+f_t^{n'}} \geq q(f_t^{n'})$ since $\phi_t^{n'} = \beta \phi_{t+1}^{n'}$.

Note that

$$\begin{aligned} m_{j,t}^{n'} &= \alpha_t^{n'} \cdot m_{j,t}^{n'} + (1-\alpha_t^{n'}) \cdot m_{j,t}^{n'} \\ &\geq \alpha_t^{n'} \cdot (1+f_t^{n'}) \cdot q(f_t^{n'}) + (1-\alpha_t^{n'}) \cdot m_{j,t}^{n'} \\ &= \alpha_t^{n'} \cdot u'\left(q(f_t^{n'})\right) \cdot q(f_t^{n'}) + (1-\alpha_t^{n'}) \cdot m_{j,t}^{n'} \\ &\geq \alpha_t^{n'} \cdot u'\left(\frac{\tilde{m}_{j,t}^n}{1+f_t^n}\right) \cdot \frac{\tilde{m}_{j,t}^n}{1+f_t^n} + (1-\alpha_t^{n'}) \cdot m_{j,t}^{n'} \end{aligned}$$

Multiplying both sides by $h_t^{n'}$ reveals

$$\begin{aligned} m_t^{n'} &\geq \min\{h_t^{n'}, \eta\} \cdot u'\left(\frac{\tilde{m}_{j,t}^n}{1+f_t^n}\right) \cdot \frac{\tilde{m}_{j,t}^n}{1+f_t^n} + (1-\alpha_t^{n'}) \cdot h_t^{n'} \cdot m_{j,t}^{n'} \\ &> \min\{h_t^n, \eta\} \cdot u'\left(\frac{\tilde{m}_{j,t}^n}{1+f_t^n}\right) \cdot \frac{\tilde{m}_{j,t}^n}{1+f_t^n} + (1-\alpha_t^n) \cdot h_t^n \cdot m_{j,t}^n \\ &= m_t^n \end{aligned}$$

which completes the first part of the proof.

To show that $m_t^n < m_t^{n'}$ only if $\pi_{t+1}^n > \pi_{t+1}^{n'}$, suppose $\pi_{t+1}^n \leq \pi_{t+1}^{n'}$ and follow the same steps as above. This completes the proof. □

G.4 Proof of Proposition 9

Proof. Consider $n \in \mathcal{M}$, $n \notin \tilde{\mathcal{N}}$, and $n' \in \tilde{\mathcal{N}}$. Let $\mu^n > \mu^{n'}$. Real coin n' balances are now given by

$$m_t^{n'} = min\left\{\hat{m}_t^{n'}, \underline{m}^{n'}\right\}$$

where

$$\hat{m}_t^{n'} = min\{h_t^{n'}, \eta\} \cdot u'(\tilde{m}_{j,t}^n) \cdot \tilde{m}_{j,t}^{n'} + \left(1-\alpha_t^{n'}\right) \cdot h_t^{n'} \tilde{m}_{j,t}^{n'}$$

Coin n real balances are given by $m_t^n = \hat{m}_t^n$.

First suppose that $m_t^{n'} = \hat{m}_t^{n'}$ for at least one $t \geq 0$. Consider the relative aggregate real coin

balances that evolve according to

$$\frac{m_{t+1}^n}{m_{t+1}^{n'}} \;=\; \frac{1+\mu^n}{1+\mu^{n'}} \cdot \frac{1+\pi_{t+1}^{n'}}{1+\pi_{t+1}^n} \cdot \frac{m_t^n}{m_t^{n'}}$$

If $\pi_{t+1}^n \leq \pi_{t+1}^{n'}$, then $m_t^n \geq m_t^{n'}$. Since $\mu^n > \mu^{n'}$, it again follows that $m_{t+1}^n > m_{t+1}^{n'}$, which in turn implies that $\pi_{t+2}^n < \pi_{t+2}^{n'}$. But then $\frac{m_{t+2}^n}{m_{t+2}^{n'}} > \frac{m_{t+1}^n}{m_{t+1}^{n'}}$ which implies $m_{t+2}^n > m_{t+2}^{n'}$, which requires $\pi_{t+3}^n < \pi_{t+3}^{n'}$. This process continues as time progresses. It follows that the ratio $\frac{m_{t+s}^n}{m_{t+s}^{n'}}$ must continue to increase:

$$\lim_{s\to\infty} \frac{m_{t+s}^n}{m_{t+s}^{n'}} \;=\; \lim_{s\to\infty} \left(\frac{1+\mu^n}{1+\mu^{n'}}\right)^s \cdot \prod_{k=1}^{s} \frac{1+\pi_{t+k}^{n'}}{1+\pi_{t+k}^n} \cdot \frac{m_t^n}{m_t^{n'}} \;\to\; \infty$$

This is a contradiction: m_t^n is bounded, and $m_t^{n'} \geq \underline{m}^{n'} > 0$ for all $t \geq 0$. Thus, if $m_t^{n'} = \hat{m}_t^{n'}$ and $\mu^n > \mu^{n'}$, then $\pi_{t+1}^n > \pi_{t+1}^{n'}$ and hence $m_t^{n'} > m_t^n$. It follows that $m_t^{n'} = \underline{m}^{n'}$ for all $t \geq 0$ is a necessary condition for $m_t^n \geq m_t^{n'}$ for some $t \geq 0$.

Second, given the finding above, suppose that $m_t^{n'} = \underline{m}^{n'}$ for all $t \geq 0$. If $\underline{m}^{n'} > m_t^n$ for all $t \geq 0$, the result trivially holds. Hence suppose further that $\underline{m}^{n'} \leq m_t^n$ for at least one $t \geq 0$. By Lemma 4 it must be that $\pi_{t+1}^n \leq \pi_{t+1}^{n'}$; otherwise $m_t^n < \hat{m}_t^{n'} \leq \underline{m}^{n'}$. Since $m_t^{n'} = \underline{m}^{n'}$ for all $t \geq 0$, we have that $\mu^{n'} = \pi_{t+1}^{n'}$ for all $t \geq 0$. By the law of motion of relative balances we have

$$\frac{m_{t+1}^n}{m_{t+1}^{n'}} \;=\; \frac{m_{t+1}^n}{\underline{m}^{n'}} \;>\; \frac{m_t^n}{\underline{m}^{n'}} \;\geq\; 1$$

Since $m_{t+1}^{n'} > \hat{m}_{t+1}^{n'}$, it must be that $\pi_{t+2}^n < \pi_{t+2}^{n'}$. This again implies that $\frac{m_{t+2}^n}{\underline{m}^{n'}} > \frac{m_{t+1}^n}{\underline{m}^{n'}}$, and hence

$$\lim_{s\to\infty} \frac{m_{t+s}^n}{\underline{m}^{n'}} \;=\; \lim_{s\to\infty} \prod_{k=1}^{s} \frac{1+\mu^n}{1+\pi_{t+k}^n} \cdot \frac{m_t^n}{\underline{m}^{n'}} \;\to\; \infty$$

which cannot occur as $m_{t+1}^n < \infty$ for all $s \geq 0$. This is a contradiction, and the claim follows. □