Optimal Cryptocurrency Design: Seigniorage and Transaction Fees*

Michele Fabi†

June 2021

Latest version available at https://michelefabi.com/working-papers.

Abstract

This paper studies how transaction fees and seigniorage, equivalent to inflation in the cryptocurrency setting, affect miner incentives and trade congestion. Each cryptocurrency miner chooses how many new transactions to group into the next block of transactions that the miner competes to validate. The successful miner earns (i) transaction fees from traders seeking to record their transfers and (ii) the new cryptocurrency units or seigniorage created by block validation. Pro rata transaction fees encourage miners to include more transactions per proposed block but larger blocks transmit more slowly, raising the risk of invalidation. Raising the seigniorage to fee ratio reduces the number of transactions recorded per block. When miners choose small blocks, congestion levels rise and eventually trade breaks down, making the cryptocurrency unviable. This requires a minimal ratio of seigniorage to fees. Optimal cryptocurrency design maximizes trade efficiency subject to miner participation constraints and these miner incentives.

Keywords: Cryptocurrency miners, blockchain, congestion, seigniorage.
JEL Codes: E42, C73, D47.

*I am especially thankful to Matthew Ellman for guiding me with care and dedication throughout the development of this paper. I also thank Jordi Caballé, Ramon Caminal, Xavier Cuadras, Marc Escrihuela, Hanna Halaburda, Sjaak Hurkens, Joachim Jungherr, Hannes Mueller, Chara Papioti, Amedeo Piolatto, Hugo Rodriguez and in general IAE and UAB staff for valuable discussions. I also thank the audience at EARIE2021 and JEI2021. I gratefully acknowledge financial support - FPI fellowship 914886-79792965 - from Barcelona GSE and the Spanish Ministry of Science, Innovation and Universities (MCIU).

†Ecole Politechnique, CREST, IP Paris (michele.fabi@ensae.fr)

1 Introduction

A cryptocurrency is a digital currency governed by a computer program and managed by a decentralized, free-entry network of record-keepers in charge of updating the *blockchain*: a ledger (registry) of the collective memory of the cryptocurrency, i.e. "who-owns-what". In most cryptocurrencies, e.g. Bitcoin and its successors, record-keepers are *cryptocurrency miners*; individuals that own a dedicated computer. Miners record a *block* (or set) of pending transactions from consumption good traders (buyers and sellers) by first performing a costly encryption that makes the blockchain secure and then transmitting the block to the miner network for its approval. In case two or more blocks record conflicting information, miners coordinate on the first transmitted block and discard the others. As a compensation for the cost of recording blocks, the protocol rewards miners with revenues from two policy instruments: per-transaction fees and seigniorage from the creation of new coins. Seigniorage is the only source of revenues from empty blocks that record no transactions and only create money. By increasing block size recording more transactions, fee revenues rise while seigniorage is fixed, but block transmission time reduces; hence, also the risk of block invalidation causing the loss of its associated revenues increases. This paper studies the effects of seigniorage and transaction fees on miner incentives and trade congestion. My model shows that the size of miner blocks depends positively on the ratio of fees to seigniorage. Hence, transaction fees cannot be fully substituted by seigniorage as they are essential to induce miners in creating large blocks so to maintain a high transaction speed. Also, sufficient seigniorage is needed for positive miner activity when no trader transaction is pending. So an optimal cryptocurrency design uses both policy instruments.

Large blocks imply a short payment settlement period encouraging consumption good buyers to pay sellers using the cryptocurrency. Conversely, small blocks cause the queue of pending cryptocurrency payments to become congested and sellers to charge higher prices for the wait. In my model, excessive seigniorage causes miners to form only empty blocks, without fulfilling their primary record-keeping task. As a result, transactions have an infinite validation time, and cryptocurrency trade unravels. Congestion risks in cryptocurrency trade are evident from Bitcoin data. Figure 1 shows that most Bitcoin traders suffered long payment settlement delays in periods of high congestion, as the median confirmation time is often below the spikes occurring in the average confirmation time. In particular, during the first quarter of 2018, transactions took on average more than two days before being included in a block. Taking into account that Bitcoin traders wait for other five blocks to arrive before considering a payment safely received, payments took on average more than a week during that period of time, and caused traders to switch to alternative payment methods such as Paypal transfers.[1]

[1]On October 21 2020 Paypal announced to plan extending its service to allow trans-

[Fig. 1 about here.]

The basic mining incentive problem can be tackled by an optimal cryptocurrency design that provides miners with the efficient combination of transaction fees and seigniorage conditional on inducing sufficient miner entry for traders to consider the cryptocurrency secure. In this case, the social planner (a team of expert software developers) elicits "mining taxes" from consumption good traders in the form of inflation and transaction fees to incentivize miners in providing public goods; in particular, security from their participation, a pure public good, and block size, a common-pool good subject to congestion. Chiu and Koeppl (2019) (CK hereafter) argue that a pure seigniorage design is optimal based on the observation that seigniorage is levied on aggregate value of the cryptocurrency while transaction fees apply only to the portion of value used for trade. The larger "tax base" on which seigniorage is charged can let the protocol provide a given level of mining revenues imposing lower mining costs on traders than the ones implied by including a fee component in the block reward design. However, CK's rationale neglects the detrimental effect of excessive inflation on block size that my paper explores. My analysis shows that an equilibrium in which cryptocurrency trade takes place is viable only if the protocol ensures that transaction fees are large enough relative to seigniorage so that miners are incentivized to fulfill their role of record-keepers.

My model is the first to jointly analyze congestion and miner incentives within a general equilibrium model of trade. Hence, my contribution to the Economics literature on blockchain and cryptocurrencies is threefold. First, I encompass a game-theoretic model of block mining within a state-of-the-art, continuous-time Lagos-Wright (LW) model, in this way endogenizing token demand and inflation. Then, I use the model to derive testable implications of the sensitivity of mining strategies and trade to shifts in policy variables; in particular, the mining fees-to-seigniorage ratio. Finally, I study optimal cryptocurrency design and contribute to the debate on the composition of the block reward in terms of seigniorage and transaction fees. The analysis is roughly consistent with the stylized facts on the co-movement between blocks' size and the fees-to-seigniorage ratio that emerges from the data (e.g. Fig. 2) and opens the way for further empirical investigation. Moreover, the main lessens form the model apply to the myriad of "altcoins" (alternative cryptocurrencies) that proliferated extending the open-source Bitcoin code.[2]

fers of bitcoins and other cryptocurrencies across its accounts. For further information, check https://newsroom.paypal-corp.com/2020-10-21-PayPal-Launches-New-Service-Enabling-Users-to-Buy-Hold-and-Sell-Cryptocurrency

[2]An altcoin can be created by downloading and modifying the source code of the up-to-date version of Bitcoin Core from this link: `https://bitcoin.org/en/bitcoin-core/`.
Currently, the market capitalization of the more than 2800 different cryptocurrencies is around 200 million USD. Bitcoin is the market leader, accounting for 67% of the overall value with a capitalization of 133.43B. Ethereum and XRP (also known as Ripple) share the podium with market caps of 18.7B (9%) and 8.7B (4%) followed by the other top ten currencies (Tether, Bitcoin Cash, Bitcoin SV, Litecoin, EOs, Binance Coin, Tezos). A myriad of minor currencies constitute the remaining 7% of the total market

[Fig. 2 about here.]

The rest of this paper is organized as follows: Section 2 provides a literature review. Section 3 models the cryptocurrency-trade economy and the blockchain, describing in detail the determinants of the block invalidation risk. Section 4 presents a game-theoretical model of mining and a partial equilibrium model of cryptocurrency trade. Cryptocurrency token prices are determined by the (general) monetary equilibrium of the economy presented in Section 5. Section 6 formulates the optimal cryptocurrency design problem and provides an intuitive suggestion on the composition of the block reward with a simple example. Concluding remarks and directions for further research are presented in Section 7. Omitted derivations and proofs are presented in Appendices A and B. Appendices C and D provide a summary of the main notation and technical terms.

2 Literature review

My paper contributes to the vibrant Economics literature on blockchain and cryptocurrencies. I develop a novel approach that encompasses endogenous block size, trade congestion, money demand and monetary policy within a general-equilibrium pure cryptocurrency economy based on the cutting-edge continuous-time adaption of the Lagos-Wright (LW) model proposed by Choi and Rocheteau (2020c) - CR hereafter. Lagos et al. (2014) provides a thorough review of the new monetarist economics literature of which CR is part.

Endogenous block size, congestion and inflation have already been studied separately and to some degree by other authors; yet, to my knowledge, the analysis of their interplay is new. In the closest paper to mine, Chiu and Koeppl (2019) develop a dynamic general equilibrium model of Bitcoin adoption where buyers (who are also miners) can engage in frauds by committing double-spending (DS) attacks. CK assume a fixed block size and show that the plausibility of DS attacks imposes a minimum requirement on miner participation and pins-down a compensation level that an optimal design has to guarantee.

CK advocate for a blockchain design based on a pure seigniorage block reward since it is more efficient in collecting revenues from traders than fees, but neglect congestion (see Section 1). CK also point out that fees can be reclaimed after a successful double-spending so that they provide a less effective DS deterrent than seigniorage. Nevertheless, in practice fees are small relative to the transaction value that justifies a DS attack and have only a minor effect on DS incentives. My story based on congestion and endogenous block size provides a rationale for adding a fee component to the block reward.

Houy (2016) along with the Computer Science paper Rizun (2015) is one of the earliest contributions on endogenous block size with a model of the invalidation risk. He assumes

value-the majority of each has a value share lower than 1%.

continuous block size and also finds that block size is increasing in the fee-to-seigniorage ratio, in line with my findings. My paper augments the existing block size game by also studying miner activity and entry and also by endogenizing cryptocurrency trade. Earlier contributions miss modeling mempool dynamics resulting from the general equilibrium of the economy, which are an important link between mining and trade.

Huberman et al. (2019) and Easley et al. (2019) - HLM and EOB - offer an in-depth analysis of Bitcoin transaction fees. I focus instead on analyzing the optimal trade-off between fees and seigniorage, abstracting from the fee auction modeled by these authors and assuming homogeneous users and a fixed posted price as fee set by the protocol.[3]

Even though the models developed by EOB and HLM are suited to address the determination of fees, they treat trade as exogenous and assume linear impatience. This feature precludes a direct dynamic extension as standard models assume negative exponential discounting. On the other hand, CK endogenize trade and embed a game-theoretic model of mining within a LW monetary model in discrete time. This approach is suited for optimal cryptocurrency design but is not compatible with the continuous-time mining games studied by EOB and HLM; hence cannot be used to study congestion. My paper combines mining and monetary aspects within a continuous-time framework. As in EOB, I restrict the maximum block size to unity when investigating miners' optimal block size strategy. The novel mining aspect I consider is the trade-off between block reward and invalidation risk. HLM propose a modified Bitcoin protocol that adjusts block size and creation rate based on transaction demand. Block size is fixed by the protocol and miners do not take into account the risk of block invalidation.

Fernández-Villaverde and Sanches (2019) study a general equilibrium monetary model to examine market outcomes and welfare under (Hayekian) competition among private monies produced by profit-maximizing entrepreneurs. Similarly, Choi and Rocheteau (2020c,a) develop a monetary equilibrium model in which monies are created via costly (mining) technology. These authors find that stationary equilibria with steady-state inflation, in line with the approach I employ, exist. These equilibria are part of a multiplicity set featuring, for example, boom and burst dynamics and persistently declining purchase power. Schilling and Uhlig (2019) study a two-currency economy in which the US dollar and Bitcoin coexist. They determine a condition that rules out Bitcoin speculation and ensures that BTC price (in USD) follows a martingale. Specifically, Bitcoin speculation does not occur if agents are sufficiently impatient. Athey et al. (2016) develop a general equilibrium model of remittances to endogenize the Bitcoin price.

Biais et al. (2019), preceded by the Computer Science paper Kroll et al. (2013), use a stochastic game to investigate miners' fork resolution strategies. They demonstrate that LCR is an equilibrium mining strategy but coordination effects lead to multiplicity of equilibria, some of them portraying permanent forking. Their paper includes an

[3]"Users" in HML and EOB are replaced by "traders" in my model.

extension of the baseline model with delays in information transmissions, akin to the block transmission delays considered here, showing, in agreement with my analysis, that information delays can lead to temporary forks. The main modeling difference is that, in Biais et al. (2019), blocks are transmitted instantaneously to all miners except in one - and only one - transmission that can fail to reach a miner. In that case, the uninformed miner creates a fork as a result of the information asymmetry. In my model, blocks have different transmission times depending on their size, but completed block transmissions reach all miners at once. With my modeling approach, forking is caused by differences in transmission times. I first provide a detailed description of how LCR leads miners to discard (fork-out) blocks that have been transmitted slowly and then compute, in some cases explicitly, the probability of blocks becoming stale.

Prat and Walter (2018) estimate industry dynamics of Bitcoin mining contributing to the literature on irreversible investment and explaining price dynamics. They assume exogenous token demand and abstract from block reward design. Cong et al. (2019) provides an analysis of the industrial organization of mining pools.

Other papers, e.g. Abadi and Brunnermeier (2018); Leshno and Strack (2019); Saleh (2020); Rosu and Saleh (2019) are broadly related to mine and discuss general aspects of blockchain ecosystems and the Proof-of-Stake (PoS) protocol, the leading alternative to Proof-of-Work (PoW). In particular, Budish (2018) criticizes the blockchain technology highlighting potential vulnerabilities of the infrastructure to DS and other types of attack.

My paper also relates to the Computer Science literature on blockchains. Decker and Wattenhofer (2013) describe in detail the block propagation method used by Bitcoin miners and measure blocks propagation time on the Bitcoin blockchain. I refer to invalid blocks as "stale" according to the definition provided by Saad et al. (2019). Neudecker and Hartenstein (2019) study empirically temporary forks originated by block propagation delays. Carlsten et al. (2016) argue that a pure fee reward creates security breaches. In particular, random shifts in transaction fees caused by stochastic demand can cause mining revenues to fall below mining costs, thereby discouraging miner participation. This happens for example when no transaction is pending for validation so that miners make no revenues from mining. Rosenfeld (2014); Pinzón and Rocha (2016); Grunspan and Pérez-Marco (2018) compute the success probability of a double-spending attack refining the calculations reported in Nakamoto (2008).

3 Model

REPLACE permanent with MAXIMAL mining

My model augments the novel continuous-time LW framework proposed by Choi and Rocheteau (2020c) with an explicit model of blockchain mining, featuring endogenous block space.

The economy is populated by B buyers, S sellers and M miners, indexed by b, s, m respectively. Traders' (buyers and sellers) participation is exogenous, while miner participation will be determined endogenously by free entry. I denote the time index $t \in \mathbb{R}_+$.

Two types of perishable and divisible goods are available in the economy. The first is a generic (numéraire) good denoted by $x \in \mathbb{R}$, with $x > 0$ if consumed and $x < 0$ if produced, that can be interpreted as a basic consumption good if positive or as labour if negative. The second is a special good whose consumption and production is denoted by $y \in \mathbb{R}$—it can be interpreted as a consumption good that is augmented with special features if purchased from an E-commerce website via cryptocurrencies. All agents enjoy consuming the generic good (and dislike producing it) according to the same one-to-one utility function, so the payoff they obtain by consuming or producing x is simply given by x. Preferences for the special good are instead asymmetric. Buyers cannot produce the special good but do enjoy consuming it according to the generalized logarithmic utility

$$u(y) = \ln(1 + \eta\, y), \quad \eta \in \mathbb{R}_+ \tag{1}$$

This functional form was first introduced in its more general form of generalized CRRA utility in Lagos and Wright (2005) and then employed by Chiu and Koeppl (2019) to normalize utility such that $u(0) = 0$ and to avoid a corner solution with no trade when even optimal consumption would yield a negative utility.[4] The taste parameter η is needed and has to be sufficiently large to solve this issue.

Sellers instead can produce the special good but do not enjoy consuming it, while miners are neither able to produce nor interested in consuming the special good.

All agents can also obtain storable and perfectly divisible tokens of a PoW cryptocurrency with no intrinsic consumption value, i.e. a fiat cryptocurrency. In Bitcoin, tokens are called "bitcoins" and "satoshis," (a bitcoin is worth 10^8 satoshis).[5] I let $a_{i,t}$, $i \in \{b, s, m\}$ denote the tokens held by agent i and $z_{i,t} \equiv a_{i,t}\phi_t$ their real value given price ϕ_t.

3.1 Centralized markets (CM's)

Only miners can produce cryptocurrency tokens. Nevertheless, all agents can obtain and dispose of tokens through centralized cryptocurrency markets (CM's). Specifically, two trading platforms, CM_1 and CM_2 (e.g. Coinbase and Binance), are continuously and simultaneously acting as market makers, allowing agents to exchange tokens for units of the generic good and vice-versa.

[4] The generalized CRRA used in Lagos and Wright (2005) is equivalent to $u(y) = (1-\epsilon)^{-1}[(y + 1/\eta)^{(1-\epsilon)} - (1/\eta)^{(1-\epsilon)}]$, which converges to the utility function (1) for $\epsilon \to 1$.

[5] Fiat currency sometimes is interpreted as money backed by the government and issued by a central bank. I refer to these as *traditional* fiat currencies. Here, by "fiat currency" I refer to an asset that yields no dividends as opposed to a Lucas tree.

Besides being exchanges, the CM's allow traders to subscribe and opt for a token custody service. In this way, while retaining the tokens' ownership, traders let a CM store their tokens in compliance with the Know Your Costumer (KYC) and Anti Money Laundering (AML) regulations. Trading platforms perform the custodial service by providing traders with a *custodial wallet* that they can use to manage their funds. In this model, all traders opt for the custody service and operate only trough their custodial wallets. Miners instead keep their tokens "in their own hands" on a non-custodial wallet. To keep things simple, I assume all traders single-home and each CM interacts with half of the traders' population. Formally, denoting a CM's user base with sub-index, I am making the following assumption:

Assumption 1. $(B_1, S_1) = (B_2, S_2) = (B/2, S/2)$

Miners instead operates with both CM's.

Each CM performs two types of operations: internal transactions, among and with her subscribed traders, and external transactions, encompassing those among subscribed and unsubscribed traders and miner-platform transactions. Transactions of this last category take place after miners recorded them on the blockchain in a valid block, i.e. they are *on-chain* transactions. In this case, their settlement is not immediate, and record-keeping is in general not final because, once a block becomes stale, the transactions it records turn to be pending again. Conversely, internal transactions are performed using a double-layer solution that does not rely on the blockchain; i.e. they are *off-chain* transactions. To perform transactions of this category, first, a CM forms a centralized fund buying tokens via external transactions—at first buying from miners and later also from unsubscribed traders. Afterwards, she lets subscribed traders access a limited part of her fund ($a_{b,t}$ and $a_{s,t}$ to a generic buyer and seller) through their custodial wallets. In this way, internal transactions only update traders' wallet balance, but de facto do not move tokens across addresses. Thanks to this procedure, internal transactions achieve immediate and final settlement.[6]

All external transactions experience settlement delays, but I assume that miner-to-platform operations are immediate, as considering the effect of their settlement delays would only complicate the model without making it further insightful.

3.2 Decentralized market (DM)

Besides trading in the CM's, traders also meet sporadically among each other in a decentralized market (DM). Given the preference and technology asymmetry among buyers and sellers, DM meetings are the only occasion for buyers to purchase the special good

[6]Indeed, the Bitcoin blockchain explorer https://www.blockchain.com/explorer does not record transactions made through Coinbase wallets, as explained in Coinbase FAQ (frequently-asked-questions).

from sellers. I let $\alpha_{i,j}$, $i,j \in \{1,2\}$ denote the (Poisson) meeting rate among CM i buyers and CM j sellers.

Since the custodial wallets are incompatible across CM's, DM transactions among traders of different platforms occur *on-chain*; precisely, when a transaction takes place, the buyer requests his trade platform to send a number of tokens to the seller's address, which points to his trading platforms. In this model, a precise analysis of blockchain record-keeping is pointless unless traders with incompatible wallets meet with positive probability. So, to keep things tidy, I assume that DM meetings occur *only* among buyers and sellers with incompatible wallets, as stated by the following assumption.

Assumption 2. $\alpha_{1,2} = \alpha_{2,1} \equiv \alpha, \quad \alpha_{1,1} = \alpha_{2,2} = 0$

During DM meetings, I assume that credit is ruled out by market practices or anonymity - e.g. if special good is illegal, traders identify themselves using an encrypted alias.[7] Assuming that buyers cannot produce the generic good while trading with sellers, the only way they can obtain the special good is by exchanging it for their cryptocurrency tokens. This feature makes the cryptocurrency essential, in the sense that it widens the frontier of welfare-improving trade arrangements.

To reward miners for recording DM transactions on the blockchain, traders' wallets are programmed to charge a transaction fee for each transaction made. I assume that wallets charge a proportional transaction fee rate τ on each transaction. To be clear, if buyer b sends tokens of value $z_{b,t}$ to seller s, this latter receives only $z_{s,t} = z_{b,t}(1-\tau)$. The miner m that records the transaction between b and s in a valid block receives $z_{m,t} = z_{b,t}\tau$ real balances in reward for doing so.

In reality, buyers set the amount of fees attached to their transactions. Here, by considering τ as fixed, I give up some realism for the sake of simplicity. The model provides the simplest yet parsimonious setting to study the general equilibrium implications of a change in transaction fees.

Transaction fees are not the only source of rewards for miners and currently constitute only a minor component of it. The most important part of their reward comes from seigniorage in the form of new tokens that are generated by the protocol each time a miner forms a valid block. I postpone this aspect to Section 3.4 that describes the details of tokens' creation and the composition of the block reward.

[Fig. 3 about here.]

Market clearing and symmetry

Each CM sets her token price $\phi_{i,t}$ to ensure market clearing at each date and for each realization of (tokens) demand and supply shocks. Formally, letting $(A^D_{i,t}, A^S_{i,t})$ denote

[7] Even in these cases traders' identity can be retrieved indirectly by analyzing the blockchain tree. For example, The FBI was able to trace the identity of most people involved in illicit trade through the website Silk Road.

CM i's token demand and supply, market clearing implies

$$\phi_{i,t} : A^D_{i,t} = A^S_{i,t} \equiv A_{i,t} \quad \forall\ i,t \tag{2}$$

The resulting aggregate real value of tokens is

$$Z_t \triangleq \phi_{1,t} A_{1,t} + \phi_{2,t} A_{2,t}$$

In the monetary (general) equilibrium characterized in Section 5, the token demand in each CM is constant - except at zero-measure time points - but the token supply is subject to shocks. Specifically, positive supply shocks occur each time a CM receives tokens from a miner-platform or DM transaction, while negative supply shocks occur every time a CM gives away her tokens in a DM transaction. Nonetheless, in expectation, the symmetry Assumptions 1 and 2 imply that DM shocks compensate each other across CM's. Therefore, CM's expected prices are equal and are determined by the (constant) tokens' demand and miners' token supply. Since traders' portfolio choice and mining strategies are based on the same expected price, we can without loss of generality drop the CM index when analyzing the partial equilibrium models of mining and cryptocurrency trade developed in Section 4, basing the analysis on a single price ϕ.[8]

The aggregate number of tokens in circulation varies over time, but the general equilibrium I will characterize in Section 5 has the property that aggregate real balances are constant in each CM.

Definition 1 (Stationarity property)**.** *Aggregate real balances are stationary at CM level if*

$$Z_{i,t} = Z_i \quad \textit{for } i = 1, 2 \tag{3}$$

and for all $t \in \mathbb{R}_+$ except for a set of dates with zero Lebesgue measure.

The equilibrium describes a situation in which tokens' (expected) price is on a steady inflation path and is not subject to speculative bubbles. In reality, BTC price volatility caused by speculation raises major concerns regarding the use of BTC as a means of payment (MoP). The two-platform structure of the model is suited for analyzing cryptocurrency speculation, but in this draft, I concentrate on the hypothetical scenario in which problems arising from speculation are resolved.

Summary

To conclude this section, I recap how cryptocurrency tokens and consumption goods circulate in the economy as illustrated by Fig. 4. In type-(i) exchanges, miners sell

[8] As in reality, realized prices can temporarily differ despite the symmetry assumptions, providing agents with arbitrage opportunities. However, arbitrage is not worthwhile if its expected gains are offset by the hassle cost of monitoring both CM's at the same time. I will take his aspect for granted hereafter.

their block rewards to the CM's in exchange for generic goods. In the ones of type-(ii), buyers acquire tokens from CM's by selling units of the generic good and use their tokens to trade with sellers in the DM where type-(iii) exchanges take place: a share of the value transferred in DM meetings goes a sellers (iii.a); the remaining part goes back to a miner in the form of transaction fees (iii.b).[9] Type-(iv) exchanges occur as soon as DM transactions are recorded on a valid block, so that sellers cash-out their tokens by selling them in the CM in exchange for units of the generic good.

[Fig. 4 about here.]

Understating the internal mechanisms ruling the blockchain is essential for studying the general equilibrium of the cryptocurrency economy. For this reason, the next section presents a detailed model of blockchain mining that complements the trade framework presented up to now.

3.3 The blockchain

The blockchain is a digital ledger that records all movements of cryptocurrency tokens directed towards each user address as well as modifications of the token creation policy and in the ledger's internal governance. The kind of blockchains studied in this paper are based on the PoW protocol that puts miners in charge of three fundamental tasks: record-keeping, consensus formation and security.

Each miner stores a copy of the ledger on his mining node and records incoming transactions sent by traders. Transactions are recorded on a miner's blockchain copy in time-stamped batches called *blocks*. To form blocks, a miner is required to solve a computationally-intensive cryptographic puzzle through random guessing of its solution, an operation called *mining* that nowadays requires a dedicated ASICS hardware to be performed.[10] In reward for mining, miners receive seigniorage from the creation of new tokens and fees associated with each transaction they record.[11]

The costly PoW requirement exists for two main reasons. The first is to give value to the cryptocurrency by making its supply costly, as the consequences of removing the PoW mechanism on the value of the cryptocurrency are analogous to those of letting people print M0 and M1 money (basically coins and banknotes) with their home printer on the value of a traditional fiat currency. The second role is related to security, but I delay this aspect after having described the structure of a blockchain in the paragraphs

[9] Technically, transaction fees resulting from the difference between the number of tokens sent from an address and that directed to the other address or addresses.

[10] ASICS is an acronym for Application-Specific Integrated Circuit System. ASICS mining nodes were anticipated first by computational processing units (CPU's), and then by graphical processing units (GPU's).

[11] An alternative blockchain protocol is Proof-of-Stake (PoS) which replaces miners with "validators," who are required to form a token escrow fund and obtain the right to record blocks if extracted by a lottery that selects them based on their relative contribution to total token escrow.

below.

Due to the distributed nature of blockchain record-keeping, miners are naturally prone to record different transactions histories to their ledger copies. For example, if miners form blocks by recording pending transactions at random, their ledger copies can differ in the chronological order in which transactions are recorded. Nevertheless, the governance rules followed by miners have to ensure that miners reach an agreement on a common version of the ledger by communicating to each other the blocks they recorded and pending transactions they store, allowing only for temporary inconsistencies among their ledger copies.

In the next subsection, I will provide a brief description of the structure of a blockchain and the miner governance rule adopted by Bitcoin and most PoW cryptocurrencies. The following short description suffices to follow the mining model developed in Section 4.1. Other minor mining technicalities are presented in Appendix D.

The structure of a blockchain (in brief)

A blockchain is formed by connected blocks of recorded transactions and auxiliary information. Each blockchain is initiated by a genesis block that is progressively extended by its successors establishing a chronological order. Asynchronous and decentralized communication among miners can lead them to extend a single block by two or more direct (chronological) successors. In this case, the blockchain *forks* (bifurcates) in two or more chains (branches), each providing a different version of the ledger up to a common point of agreement. Due to possible forking, the correct model to keep track of the blockchain's ramification is that of a directed tree graph, usually referred to as the *block tree*, described rigorously by Biais et al. (2019). Identifying a block's precise location within the block tree requires modeling techniques that are not necessary to develop the analysis that follows. Hence, I identify each block only by the identity of the miner m who forged it and a block height $h \in \{0, 1, \ldots, H_t\}$ that counts its block distance from the genesis block ($h = 0$). The variable H_t indicates the blockchain height (i.e. the height of the block head of the longest chain). I omit the time index from H_t when clear form the context or referring to a generic value H of the blockchain height. I also refer to a chain's height as the height of its block head.

Each chain (branch) of the block tree is initiated either by the genesis block or by a fork and portrays a different history of the ledger. For this reason, the presence of multiple active chains create ambiguity on the state of the ledger, e.g. on the balance associated with each cryptocurrency address, and hinders users' trust in the blockchain if persistent. To avoid a state of permanent ambiguity, the governance rules followed by miners have to guarantee that they "form a consensus" over a unique chain to extend, allowing for simultaneous active chains only temporarily.

Bitcoin and most (if not all) PoW blockchains follow the chain selection criterion prescribed by Nakamoto (2008); namely, the Longest-Chain-Rule (LCR). Essentially, LCR prescribes miners to consider as valid the *perceived* longest chain by electing its block head (terminal block) as reference (predecessor) block for the new block they will form. If a single block has height H, miners following LCR form their new block on top of it. On the other hand, if the blockchain terminates with a fork (multiple blocks have height H), miners work on the terminal block they became first aware of; that is, on the block with the shortest *publication time* (the stopping time at which it is recorded on the ledger and transmitted to the miners' network). Put differently, miners following LCR behave as if they were to choose their favourite chain according to a lexicographic preference, with chain height as primary criterion and publication time of a chain's block head as subordinate criterion.

Under LCR, a miner m^* extends the blockchain at height H establishing the new consensus chain (at height $H+1$) by publishing a block with the shortest publication time T_{H+1,m^*} among the ones of all the miners $m \in \mathcal{M}$ that are simultaneously competing to extend the longest chain. Formally, LCR determines the reference block as follows:

Criterion 1 (LCR)**.** *Under the Longest-Chain-Rule (LCR), a miner m^* establishes the consensus chain at height H if*

$$T_{H+1,m^*} = T^*_{H+1} \triangleq \min \left\{ T_{H+1,m} \right\}_{m \in \mathcal{M}} \tag{4}$$

[Fig. 5 about here.]

From the perspective of a miner following LCR, all blocks outside the consensus chain are *stale* and do not contribute to the ledger's recorded history of transactions.

LCR is a natural prescription under transaction homogeneity. If we depart from this benchmark case, there are reasons to believe that rational miners can follow a different behaviour. For example, with heterogeneous transaction fees, Carlsten et al. (2016) shows mining equilibria such that miners extend the branch whose terminal block provides them with the largest amount of transaction fees. Also, Biais et al. (2019) shows that LCR is a plausible mining prediction, but also that other equilibria can arise due to coordination motives, e.g. prescribing miners to extend the last longest branch they become aware of (with the longest update time) rather than the first. The same coordination motives that sustain LCR can also lead to an equilibrium with permanent forking.

Miners also deviate from LCR by intentionally forking the blockchain when committing a fraud, e.g. altering the history of recorded transactions - as in the case of history reversals, including DS attacks, described later in Section 3.4 - or when using in selfish mining strategies analyzed by Eyal and Sirer (2014).

3.4 Mining

To form a new block, a miner has to (i) select a subset of pending transactions from his mem-pool (ii) choose a reference predecessor and find a PoW for his block (iii) communicate his block successfully to the other miners.

PoW and block rate

Each miner m can generate PoW solutions at a Poisson rate μ_m determined by the hash-power (production of PoW solutions) produced by his mining rig and the PoW difficulty set by the protocol. Conversely, the (average) block creation rate

$$\mu \triangleq \sum\nolimits_m \mu_m$$

is fixed by the protocol, which scales-up the PoW difficulty based on the aggregate hash power. In Bitcoin, a difficulty adjustment is applied every two weeks to restore an average block creation time of 10 minutes based on an estimate of miners' aggregate computing power (see Fig. 6).

[Fig. 6 about here.]

Biais et al. (2019) provides a detailed description of how the difficulty adjustment is implemented. Under hash rate homogeneity, a generic miner's PoW rate as a function of the number of other active miners M is described by the formula[12]

$$\mu_m = \frac{\mu}{M} \quad \forall m \tag{5}$$

From the $1/M$ term in the above expression we can see that each miner creates a negative difficulty externality on the other miners.

For a steady-state distribution of miners' mem-pools to exist, the rate at which transactions are processed has to be higher than transaction request rate $\lambda \equiv \alpha B$. The following condition ensures that miners' mem-pools do not explode when the processing capacity they offer is maximal.

Assumption 3. $\mu > \alpha B$

Transmission delays

After finding a valid PoW, a miner can collect a block reward for his block only if it does not become *stale* in an abandoned branch of the blockchain.[13] In my model, delays in miners' communication are the only source of stale blocks.

[12] In what follows mining activity is constant over time so that also PoW rates are constant. With time-varying aggregate mining power also hash rates would fluctuate.

[13] Some authors refer to blocks outside the consensus chain as "orphan blocks". I follow Saad et al. (2019) and consider as orphan the blocks that extend an invalid predecessor.

To keep thing simple, I assume that users communicate their transaction requests instantly to all miners and each miner observes the completion time of his block transmissions, which reach all other miners simultaneously. The only communication friction is provoked by transmission delays that depend on the size of blocks. In this model, blocks are either empty or filled with one transaction only. For now, to facilitate exposition, I denote the size of a miner's block by $k_m \in \{0, 1\} \cup \{\texttt{OFF}\}$, where I use the convention that $k_m = \texttt{OFF}$ if the miner does not produce any block (his mining rig is shut down). When presenting the game-theoretic model of mining in Section 4.1 I will let miners strategize on the size of their blocks based on number Q_t of pending transactions in their mempools, so that they will set $k_m(Q_t)$ for $Q_t \in \mathbb{N}_0$.

Empty blocks are transmitted immediately, while filled blocks are transmitted after an exponentially distributed transmission lag with average $1/\theta$. I further assume for tractability that miners update their ledger copies only after the blocks they create are published (mined and transmitted). Under these assumptions and LCR (described in Section 3.3), all miners work on extending the unique consensus chain.

Apart from the case in which $k_m = \texttt{OFF}$, the time it takes a miner m to forge and transmit a new block that *extends* the consensus chain at height H is the sum of the PoW solution time $\gamma_{H+1,m}$ and transmission lag $\epsilon_{H+1,m}$ of his new block. Thus, its the publication time results from

$$T_{H+1,m} = T^*_H + \gamma_{H+1,m} + \epsilon_{H+1,m}$$

where T^*_H is the publication time of the reference block for height H. The solution time $\gamma_{H+1,m}$ is exponentially distributed with rate μ_m in accordance with Eq. (5). The transmission lag $\epsilon_{H+1,m}$ of miner m's new block depends on its size. If $k_m = 0$, its transmission is instantaneous ($\epsilon_{H+1,m} = 0$); if $k_m = 1$ its transmission lag is exponentially distributed with rate θ. The density of the total solution and transmission time when a miner fills his new block with probability σ_m is the given by the following mixture distribution:

$$f_{\gamma_{H+1,m}+\epsilon_{H+1,m}}(t) = \sigma_m \left[\frac{\theta \mu_m}{\theta - \mu_m} \left(e^{-t\mu_m} - e^{-t\theta} \right) \right] + (1 - \sigma_m)\mu_m e^{-t\mu_m} \tag{6}$$

Notice that, for $\sigma_m = 0$, density (6) becomes a simple exponential density, while in the opposite case of $\sigma_m = 1$, it becomes the density of the sum of two exponential random variables with different rates (a two-parameter hypo-exponential distribution).

Under LCR, all miners will use as next reference block the one extending the longest chain with the shortest publication time according to relationship (4). Hence, the prob-

ability that a miner m^* forms next reference block satisfies

$$\mathbb{P}\left(T^*_{H+1} = T_{H+1,m^*}\right) = \mathbb{P}\left(\gamma_{H+1,m^*} + \epsilon_{H+1,m^*} < \min_{m'}\left\{\gamma_{H+1,m'} + \epsilon_{H+1,m'}\right\}\right) \tag{7}$$

If successful, miner m^* establishes the new longest chain and causes all other blocks in transmission to become stale, each forming a separate abandoned chain. Formula (7) is employed in Section 4.1 to determine a miner's estimate of the probability of successful mining of a block given a belief on the size of the other blocks in contemporaneous transmission. Fig. 7 shows an illustrative blockchain ramification caused by three miners competing to establish the consensus chain given the characteristics of block transmission stylized in this section.

[Fig. 7 about here.]

In current cryptocurrency blockchains, information transmission is quick and encounters little geographical impediments.[14] The resulting transmission delays are of a lower order of magnitude than block creation times. To be precise, according to the estimates for Bitcoin reported in Decker and Wattenhofer (2013), $\mu \approx 1/600$ (one block creation every 10 minutes) and $\theta \approx 1/10$ (one completed transmission every 10 seconds). These numbers are in line with Fig. 6 on block creation and Fig. 8 on block propagation. Therefore, the effect of transmission lags on the block creation process can be safely ignored, as well as the probability that a miner finds a PoW before completing a block transmission.[15] Based on the previous observation, I approximate the distribution of inter-update time of reference blocks using an exponential distribution with parameter μ:

$$f_{T^*_{H+1}-T^*_H}(t) \approx \tilde{f}_{T^*_{H+1}-T^*_H}(t) = \mu e^{-\mu t}, \quad t \geq 0 \tag{8}$$

This approximation can lead to slightly different probabilities than the ones produced by the actual distribution of the inter-update time between reference predecessor blocks but does not affect any qualitative result of this paper. Moreover, it allows to solve explicitly and neatly all agents' value functions, which otherwise would be too complicated and convoluted to be handled.[16]

[Fig. 8 about here.]

In reward for successful mining, miners earn a block reward $R(k_m)$ depending on the size of their blocks, with $R(1) \geq R(0) \geq R(\mathsf{OFF}) = 0$. By choosing to record a filled rather than empty block, a miner faces a higher risk that his block becomes stale; but, if the block transmits successfully, he earns a higher reward from transaction fees.

[14] The Canadian blockchain technology company Blockstream started recently to broadcast the Bitcoin blockchain via satellite to facilitate the transmission and reception of Bitcoin data from areas with scarce or inaccessible internet services. More information is available at the following link: https://blockstream.com/satellite/

[15] A block transmission is considered completed when it reaches a certain majority of miners. Fig. 8 shows that a block reaches 90% of Bitcoin miners' population in about 10 minutes.

[16] The exact distribution of μ is the one of the minimum of M random variables with density (6).

Block reward

Each time a miner successfully records a valid block, he earns a block reward composed of seigniorage from newly created tokens and transaction fees. To award a miner with the latter, the protocol transfers new tokens to his address with a *coinbase* transaction. Metaphorically speaking, miners seek the "digital gold" contained in each valid block. Hereafter, each (valid) block contains an amount ΔA_t of new tokens, set in fixed proportion to the total token supply.

Since cryptocurrency trade occurs at sufficiently high frequency, a law of large number (LLN) ensures that trade supply shocks are neutralized at CM aggregate level. In this way, price shocks are only caused by miners selling their coinbase rewards. Throughout this paper, I let the protocol set a steady inflation rate in both CM's. Specifically, if a miner sells a coinbase transaction to the CM's at time t_+, the resulting price shock in a generic CM has a magnitude of $\phi_{t_+}/\phi_t = 1 - \pi$, where $\pi \in [0, 1]$ denotes a seigniorage rate. The protocol implements the desired seigniorage rate π by setting

$$\Delta A_t = A_t \frac{\pi}{1 - \pi}$$

Under steady inflation, the value of miners' seigniorage reward is the product of the seigniorage rate π and the stock of aggregate real balances Z_t.

$$\Delta A_t \phi_t = Z_t \pi \tag{9}$$

The block reward $R(k_m)$ combines seigniorage with transaction fees of rate τ earned on the k transactions included in a block. Given that, in equilibrium, all B buyers carry the same amount of real balances $z_t = z$, so that $Z = zB$, the total block reward amounts to

$$R(k_m) = z\left(\pi B + \tau k_m\right), \; k_m \in \{0, 1\}, \qquad R(\mathsf{OFF}) = 0 \tag{10}$$

The token creation rule presented before establishes a constant inflation rate. Bitcoin implements a staggered decreasing inflation rule such the tokens produced in each valid block are halved each time the total token production hits one of a set of predetermined target values. These events are called "Bitcoin halvings" and are programmed to impose a total supply cap of 21 million bitcoins, to be reached approximately in the year 2140.[17] After then, Bitcoin will feature block rewards made only by transaction fees and a negative inflation rate driven by tokens going out of circulation by getting lost or ending up in abandoned accounts.

The model applies to Bitcoin in a scenario where the next halving is far from agents' temporal planning horizon. It is also valid for the many cryptocurrencies based on a steady token creation rule, such as the current PoW implementation of Ethereum. It

[17] The last Bitcoin halving took place on May 11th, 2020.

does not apply to cryptocurrencies that implement a negative inflation rate by "burning tokens," sending a part of them to an irretrievable address each time a valid block is recorded.

Security

Suppose that the most extended blockchain branch has height H_t and a malicious miner deviates from LCR and attempts to re-write the information stored in a block at height, $h < H_t$. Since block identifiers are chained recursively, to succeed in doing so by time t' the hacker has to create a secret chain that re-writes all blocks at height $h' \in \{h, h+1, \ldots, H_t, \ldots, H_{t'}\}$, where $H_{t'} \geq H_t$ is the blockchain height reached during the attack, solving the PoW cumulatively, and release his branch once it surpasses the honest one. In this way, the attacker engages in a mining race with the honest miners, as he needs to keep up with the additional blocks that extend the blockchain. The likelihood that the attacker succeeds is decreasing with the participation of honest miners because it makes honest (longest) chain to grow faster. Hereafter, as in Easley et al. (2019), I assume that cryptographic attacks are ruled out if at least $\underline{M}$ (honest) miners are active. This level of mining activity is also required for traders to trust in using the cryptocurrency.

Now that all the fundamental ingredients of the cryptocurrency-based economy have been introduced, I am ready to move to the next section, in which I analyze the partial equilibrium models of mining and trade.

4 Mining and trade equilibria

In this section, I present the partial equilibrium models of mining and trade. Mining involves strategic interactions that require game-theory modeling. Essential elements for the design results discussed in Section 6 are the probability at which a given miner works on recording a block (16) and miner participation under free-entry (25). I also determine the necessary conditions for any mining activity to occur (19) and a sufficient condition for each miner to be constantly mining (20).

Cryptocurrency trade can be tackled using dynamic programming (DP) and axiomatic bargaining. I use these techniques to derive the optimal amount of special good produced by sellers (35) and buyers' token demand (36).

4.1 The mining game

Section 3.3 described the technicalities and purposes of mining and the PoW protocol. Here I develop a stochastic game to analyze miners' block size choice, use of computational power and participation to the mining network. I present its elements hereafter:

Players: M miners compete for updating the consensus chain of a blockchain recording cryptocurrency transactions.

States: Miners engage in mining rounds (or tournaments) with features varying according to a (continuous-time) Markov chain. Precisely, each round is described by a two-dimensional state, given by a number of pending transactions and a blockchain height, $(Q, H) \in \mathbb{N}_0 \times \{H_0, H_0 + 1, \dots\}$, $H_0 > 0$.

Information: A generic miner m observes his copy of the ledger continuously as well as the PoW solution time $\gamma_{h,m}$ and the transmission lag $\epsilon_{h,m}$ of all the blocks he mined and transmitted. By combining this information, the miner learns the update time of his blocks $T_{h,m}, \forall h \leq H + 1$.

The miner also observes the update times and the information contained in the blocks transmitted by other miners $T_{h,m'}$ $\forall h \leq H + 1, m' \neq m$, except for the other miners' identities. Thus, since he observes all update times, he also knows the publication time of all reference blocks T^*_h, again for $h \leq H + 1$.

Finally, the miner observes his mem-pool size $Q_{m,t}$ at each point in time. Since users-to-miners communication is simultaneous and immediate and miners update their mem-pools only when either receiving transactions or recording them in finalized valid blocks, miners' mem-pools are always synchronized, recording the same number of pending transactions $Q_{m,t} = Q_t$ $\forall m$ that I denote simply as Q when the temporal dimension is implicit.

Actions: Each miner m chooses the size of the block $k_m(Q_t) \in \{0, 1\} \cup \{\mathsf{OFF}\}$ to mine on top of the longest chain and transmit to the miners' network afterward. I adopt the convention that $k_m(Q_t) = \mathsf{OFF}$ if miner m is idle (his mining rig is switched off) when the mem-pool has size Q_t. I let $Q_{T^*_m + \gamma_m}$ denotes the state of the mem-pool by the time the miner finds a PoW for a block extending the longest chain.

Payoffs: The lifetime utility of a miner is the present value of the sum of the block rewards he earns in each mining round net of the upfront investment cost for his mining node F and a flow mining cost ψ accounting for energy and obsolescence. In formula,[18]

$$\mathcal{U}_m = \mathbb{E}\left[\sum_{H=H_0}^{\infty} e^{-rT^*_{H+1}} R\left(k_m(Q_{T^*_H + \gamma_{H+1,m}})\right) \mathbb{1}_{\{T_{H+1,m} = T^*_{H+1}\}} - \psi \int_0^{\infty} e^{-rt} \mathbb{1}_{\{k_m(Q_t) \neq \mathsf{OFF}\}} \, \mathrm{d}t\right] - F \tag{11}$$

Strategies: I focus on Markov (behavioural) strategies. Specifically, each miner m chooses the probabilities $\sigma_{m,k}(Q)$ for $k \leq Q$ of forming a blocks of size k when the mem-pool has size is Q.[19] Since $k_m(0) \in \{0\} \cup \{\mathsf{OFF}\}$ and $k_m(Q) \in \{0, 1\} \cup \{\mathsf{OFF}\}$, a strategy profile prescribing miners to stay always active ($\sigma_{m,\mathsf{OFF}}(Q) = 0, \forall Q$) boils down to specifying the probabilities

[18] It is possible to make the two cost components explicit by re-parametrizing the model. Assume mining generates electricity flow cost ψ' and drastic innovations occur at rate ι making the node obsolete. Then the flow cost of mining $\psi = \psi' + \iota F$.

[19] I do not consider strategies such as grim-trigger strategies or those prescribing cyclical behaviour.

$$\sigma_m = \mathbb{P}\left(k_m(Q) = 1 \mid Q \geq 1\right)$$

Equilibrium: The equilibrium concept I employ is symmetric Markov Perfect Equilibrium (MPE). In equilibrium, $\sigma_{m,k}(Q) = \sigma_k(Q),\ \forall m$. Of fundamental importance for the rest of the paper is the concept of *permanent mining MPE*, according to which miners are always active and fill their blocks up to their size limit, constrained by the mem-pool size if lower. Letting a Markov perfect equilibrium can be described as follows:

Definition 2 (Permanent mining equilibrium)**.** *A (symmetric) permanent mining equilibrium is a MPE of the mining game is such that miners are always active and fill blocks up to their limit, whenever possible. The strategy profile of a permanent mining equilibrium is such that, for all* $m \in \mathcal{M}$*,* $\sigma_{m,0}(0) = 1$ *and* $\sigma_{m,1}(Q) \equiv \sigma = 1$ *for all* $Q \geq 1$*.*

Mining tournaments

The set of strategy profiles that are part of a symmetric MPE can be determined by discarding dominated strategies and applying the one-shot deviation principle to detect profitable deviations.

Consider the actions of an active miner m after a new reference predecessor is found. If by that time the miner has not found a PoW for his block, he simply updates his ledger and continues working on extending the new longest chain. If instead the miner finds a PoW before that time, the miner transmits his block in the hope of establishing the new target block. The miner can claim a block reward only if successful in doing so. The miner's estimate of the probability of successful mining, $P(\sigma_m, \boldsymbol{\sigma_{-m}})$, depends on his block size strategy σ_m and his belief on other miners' block strategies, $\boldsymbol{\sigma_{-m}} = \{\sigma_{-m}\}_{-m \in \mathcal{M}/\{m\}}$ and can be evaluated using formula (7). Sometimes, this procedure does not result in closed-form expressions - e.g. when evaluating off-path beliefs resulting from a particular type of equilibrium deviation. Nevertheless, it does for the parameter configurations considered hereafter. For example, evaluated along the path of a symmetric MPE, Eq. (B.9) (in appendix) provides a neat result.

Lemma 1 (Symmetric equilibrium path)**.** *Along any symmetric equilibrium path miners have equal chances of forming the next reference predecessor block.*

$$P\left(\sigma_m = \sigma, \boldsymbol{\sigma_{-m}} = \boldsymbol{\sigma}\right) = 1/M \quad \forall \sigma \in [0, 1] \tag{12}$$

Also, for $M = 2$, Eq. (B.9) determines the estimates of the successful mining probabilities for each possible equilibrium deviation in closed form.

Lemma 2 (Successful mining)**.** *For* $M = 2$*, the probability that a miner* m *forms the next valid block given his belief* σ_{-m} *on the strategy of the other miner is*

$$P(\sigma_m, \sigma_{-m}) = \frac{2\theta + (1 - \sigma_m + \sigma_{-m})\mu}{4\theta + 2\mu} \tag{13}$$

In particular,

$$P(1;\sigma) = \frac{2\theta + \sigma\mu}{4\theta + 2\mu} \qquad P(\sigma;\sigma) = 1/2 \qquad P(0;\sigma) = \frac{2\theta + (\sigma+1)\mu}{4\theta + 2\mu} \tag{14}$$

$$P(1;0) = \frac{\theta}{2\theta + \mu} \qquad P(1,1) = P(0,0) = 1/2 \qquad P(0;1) = 1 - \frac{\theta}{2\theta + \mu} \tag{15}$$

Equilibrium block size

Here, I study under which condition a profile of equilibrium block size strategies $\boldsymbol{\sigma} = (\sigma, \sigma)$ is robust to one-shot deviations assuming miners are always active. Clearly, it makes sense to check deviations from equilibrium block sizes only for $Q \geq 1$. In this case, the expected block reward for a miner that fills a block with probability σ_m satisfies

$$\begin{aligned}\mathbb{E}_{\sigma_m,\sigma_{-m}}\left[R\left(k_m(Q)\right)\right] &= (1-\sigma_m)R(0)P(0;\sigma_{-m}) + \sigma_m R(1)P(1;\sigma_{-m}) \\ &= \frac{1}{4\theta + 2\mu}\left[(1-\sigma_m)R(0)\left(2\theta + \mu(\sigma_{-m}+1)\right) + \sigma_m R(1)(2\theta + \sigma_{-m}\mu)\right]\end{aligned}$$

Stating explicitly that $R(1) = z(B\pi + \tau)$ and $R(0) = zB\pi$, a miner's best-response correspondence takes the following form

$$\sigma_m^* = \begin{cases} 0 & \text{for} \quad \sigma_{-m} < \frac{\pi B}{\tau} - 2\frac{\theta}{\mu} \\ [0,1] & \text{for} \quad \sigma_{-m} = \frac{\pi B}{\tau} - 2\frac{\theta}{\mu} \\ 1 & \text{for} \quad \sigma_{-m} > \frac{\pi B}{\tau} - 2\frac{\theta}{\mu} \end{cases} \tag{16}$$

As we can see, the best response displays strategic complementarity because is increasing in the miner's belief on his competitor's action. The unique value $\sigma = \sigma_m = \sigma_{-m}$ such that a fully mixed strategy MPE exists lies at the intersection of miners' best-responses. In other words, it is the value that makes miners indifferent between choosing any of their actions, i.e. $\mathbb{E}_{\sigma_{-m}}[R(1)] = \mathbb{E}_{\sigma_{-m}}[R(0)]$. However, such mixed-strategy equilibrium is unstable, as a small change in a miner's beliefs makes him shift away from the mixed strategy. Given the instability of the unique equilibrium with fully mixed strategies, I focus on pure strategy equilibria only.

To determine the pure strategy symmetric MPE's, notice that miners have a profitable deviation from an equilibrium prescribing $\sigma = 1$ if $\sigma_m^* = 0$ given that $\sigma_{-m} = 1$. This requires

$$\frac{\tau}{\pi} < B\left(\frac{\mu}{2\theta + \mu}\right) \tag{17}$$

Conversely, empty blocks equilibria are ruled out if $\sigma_m^* = 1$ given $\sigma_{-m} = 0$; that is, for

$$\frac{\tau}{\pi} > B\frac{\mu}{2\theta} \tag{18}$$

Conditions (17) and (18) provide a characterization of the pure strategy equilibria based on the fees-to-seigniorage ratio. If the ratio takes substantially low or high values, equilibria prescribing miners to produce empty blocks, in one case, or filled blocks, in the other, are ruled-out. For moderate values of the ratio, the game has multiple pure-strategy MPE's. Notice that higher users-to-block-size ratio ($B/1$) and block creation rate μ make condition (17) less stringent and have the opposite effect on Eq. (18); the first raises miners' seigniorage; the latter makes mining tournaments more competitive. On the contrary, a fast transmission rate θ tightens (17) ad softens (18).

Proposition 1 (MPE's)**.** *The equilibrium size of miners' blocks is determined by the fees-to-seigniorage ratio. Assuming* $M = 2$*,*

(i) For $\tau/\pi > B\mu/2\theta$*, the game has a unique pure strategy MPE with* $\sigma = 1$*;*

(ii) For $\tau/\pi < B\mu/(2\theta + \mu)$*, the game has a unique pure strategy MPE with* $\sigma = 0$*;*

(iii) For $B\mu/(2\theta + \mu) \leq \tau/\pi \leq B\mu/2\theta$*, the game has two pure strategy MPE's with* $\sigma = 1$ *and* $\sigma = 0$ *and an unstable mixed strategy MPE* $\sigma = B\frac{\pi}{\tau} - \frac{2\theta}{\mu}$

Notice that miners have incentive to fill blocks ($\sigma > 0$) only if $\tau > 0$. In this model, positive transaction fees are necessary for a monetary equilibrium to exist. If all blocks are empty, validation times are infinite, so that no trader can benefit from using tokens and the cryptocurrency economy unravels. The situation is ruled-out when the fee-to-seigniorage ratio is high enough. Indeed, condition (18) makes mining full-blocks a *dominant strategy*, i.e. each miner prefers to mine full blocks regardless the other miners' strategies. In Section 6, I will show how the protocol can set the block reward in such a way that condition (18) holds.

In the analysis developed up to here considers an equilibrium with permanent mining; that is, $k_m(Q_t) \neq \textsf{OFF}\ \forall m, t$. It is important to recognize that miners have the incentive to stay active under certain conditions. In particular, a necessary condition for an equilibrium with permanent mining activity to exist is that miners make positive expected profits from each mining tournament. Since, along a symmetric MPE path, a miner can achieve the highest level of expected profits by recording a filled block, a necessary condition for mining to be viable is that the upper bound on the flow revenue exceeds the flow cost.

$$\frac{\mu}{M} z(\pi B + \tau) \geq \psi \tag{19}$$

On the other hand, a sufficient condition for permanent mining holds if miners prefer not to wait until recording a full block if $Q = 0$. Otherwise, in the words of Carlsten et al. (2016), an empty mem-pool causes a *mining gap*, i.e. a period of mining inactivity.

Mining gaps are precluded for

$$\pi > \frac{\psi}{zB}\frac{M}{\mu} \tag{20}$$

Clearly the previous condition is violated for $\pi = 0$. In which case, miners only waste energy by mining empty blocks. Combining this observation with the $\tau > 0$ requirement for block filling, we can conclude that an MPE with permanent mining exists only for an interior block reward design; that is, for π and τ strictly positive.

Corollary 1. *A permanent mining equilibrium exists only for $\pi > 0$ and $\tau > 0$.*

Finally, an additional factor that plays a role in the activation decision is hardware deterioration, which here is neutralized by assuming no depreciation of the mining node. If mining nodes were subject to a time-increasing hazard rate of breakdown, miners would be discouraged to stay idle also by the increasing obsolescence rate.

Mem-pool and validation time distributions

Mining strategies shape the mem-pool size distribution. In particular, since valid block are transmitted approximately at rate μ, they exit the mem-pool at rate $\sigma\mu$ and enter the mem-pool at rate $\lambda = \alpha B$. The resulting stationary distribution of the mem-pool is geometric, with a probability mass function (p.m.f.) g fully determined by the (endogenous) *load* factor ρ.

$$g(Q) = (1-\rho)\,\rho^{Q} \qquad \text{with } \rho \triangleq \frac{\alpha B}{\sigma\mu} \in [0,1) \tag{21}$$

The probabilities $g(Q), Q \in \mathbb{N}_0$ can be interpreted as the fraction of time in which the mem-pool has size Q. Thus, the quantity $1-\rho$ is the faction of time in which the mem-pool is empty. For the steady state distribution to exist, the out-flow of transaction cannot exceed the in-flow, as imposed by Assumption 3.

In Section 4.2, the terms of trade set in DM meetings are based on the distribution of transactions' settlement time, determined by miners' criterion for picking transactions out of the mem-pool. Authors - e.g. Easley et al. (2019) - mention that miners follow the ROS (random order of service) criterion when selecting homogeneous transactions; prescribing miners to form blocks by extracting transactions uniformly at random from the mem-pool.[20] Under ROS, the number of valid blocks created (and transmitted) until a pending transaction is recorded on the blockchain is memoryless; in other words, it follows a geometric distribution. The probability that a transaction has to wait for $n \in \mathbb{N}_0$ (valid) blocks until being recorded is equal to

$$d(n) = \nu\,(1-\nu)^{n-1}, \quad \nu \triangleq \sigma\frac{1-\rho}{\rho}\ln(1-\rho)^{-1} \tag{22}$$

[20] Quoting EOB: "when a miner builds a block he selects from the mem-pool at random instead of taking the transaction in the pool that has been waiting the longest as in a standard first-in, first-out queue."

The success parameter ν is the probability that a transaction is recorded in the next valid block. The derivation of the distributions (21) and (22) is presented in Appendix A.1.

Miner entry

After having solved the MPE's of the mining game and computed the mem-pool and validation time distributions, I determine miners' value function to analyze their entry decision. The mining-game is connected to the cryptocurrency economy described in Section 3, in that each time miners earn a block reward they immediately sell it to the CM's in exchange for units of the generic good.[21]

Using DP terminology, a miner's state variables are his real balances $z_{m,t}$ and the number of pending transactions Q_t in the mem-pool. His choice variables are the size of his blocks $k_m(Q_t)$ and the activation indicator for his mining node $\chi_m(Q_t)$, set based on the equilibrium Markov strategies of the mining game. The mem-pool size Q follows the stationary distribution (21) at all dates, so for $\sigma = 1$, the mem-pool is filled with at least one transaction for a fraction of time $\rho = \alpha B/\mu$, and is empty for the complementary time fraction $1 - \rho = 1 - \alpha B/\mu$. Given the stationariness of Q_t, the expectation of a future block reward when miners strategize according to permanent mining equilibrium is given by

$$\mathbb{E}_Q\left[R(k_m(Q))\right] = \frac{(1-\rho)R(0) + \rho R(1)}{M} = \frac{zB\left(\pi + \frac{\alpha}{\mu}\tau\right)}{M}$$

Taking into account that valid blocks are mined at (approximately) rate μ, we can readily formulate a miner's HJB (Hamilton-Jacobi-Bellman) equation.

Lemma 3. *Given a total participation of M miners, the value function of a generic miner m under permanent mining satisfies the following equations*

$$W_M^m(z_{t_0,m}) = z_{t_0,m} + W_{0,M}^m \tag{23}$$

$$W_{0,M}^m = \frac{1}{r}\left[\frac{\mu}{M} \times z\left(\pi B + \tau\left(\frac{\alpha B}{\mu}\right)\right) - \psi\right] - F \tag{24}$$

The interpretation of Eq. (24) is straightforward. A miner makes an up-front investment F to purchase his mining node. Afterwards, he incurs a flow cost mining ψ and receives a flow revenue from block rewards $\mu\mathbb{E}_Q\left[R(k_m(Q))\right] = \frac{Bz(\mu\pi+\alpha\tau)}{M}$.

Lemma 3 can be used to study miner participation under free-entry. In this case, miners join the blockchain until all mining rents are exhausted. Given that miners enter

[21] In practice, Bitcoin miners are advised to wait for the consensus chain to extend by at least 100 additional blocks (16 hours approximately) before selling a coinbase reward, so to be confident that their blocks do not become stale.

the economy with just as needed to purchase the mining node, their lifetime utility is simply given by W_0^m. so, under free entry,

$$M^* = \sup\left\{M \in \mathbb{N} : W_{0,M}^m \geq 0, W_{0,M+1}^m < 0, \ \forall m\right\}$$

Corollary 2 (miner participation)**.** *Under free-entry, a permanent mining equilibrium features a miner participation determined by the ratio of mining revenues to costs,*

$$M = \lfloor \tilde{M} \rfloor \qquad \tilde{M} \triangleq \frac{Bz\left(\mu\pi + \alpha\tau\right)}{\psi + rF} \tag{25}$$

Traders' trust in the blockchain depends on its security level, which increases with miner participation. To ensure a secure participation level, traders require $M \geq \underline{M}$. The problem of setting the optimal block reward to induce a given level of miner participation is studied in Section 6, where I will present a simple design for $\underline{M} = 2$.

4.2 Trade

In this section, I analyse the partial equilibrium model of trade that determines buyers' optimal (cryptocurrency) portfolio choice and traders' DM bargaining conditions. Sellers are passive except when setting the terms of trade. The HJB equations that solve traders' DP problems are again presented in Appendix B.

Buyers

Each buyer can continuously trade in her CM if not busy in a DM meeting. A buyer b participating to her CM with a stock of real balances $z_{b,t}$ chooses to supply $x = -(z^* - z_{b,t})$ units of the generic good to adjust her real balances to a desired level z^*. Also, at a Poisson rate α, she engages in a DM meeting with a (randomly drawn) seller s. If the seller is available, CM trade is interrupted by a DM meeting in which b trades her tokens for units of the special good produced by s. The number of sellers is large enough to ensure that buyers almost always meet an available seller, so the total rate of DM meetings is $\lambda = \alpha B$.

In what follows, buyers can perfectly observe the blockchain and adopt the portfolio strategy of maintaining their real balances at the desired level z^* until they enter a DM meeting. To do so, buyers make a tiny adjustment in their token portfolio each time a block is produced to compensate for the inflation shock caused by a miner selling the associated coinbase. To be precise, if a buyer has z real balances before a coinbase reward is sold to the CM's, their value drops to $z(1-\pi)$ afterwards. Thus, to maintain a desired amount z^*, she has to acquire a value of $z^*\pi$ from her CM.[22]

[22]It would be more natural to assume buyers cannot observe the blockchain and let them set a

According to a DP formulation, the state variable of a buyer is given by her real balances $z_{b,t}$ and her control variable by the desired amount of balances z^* held until the next DM meeting occurs, or analogously by her generic good supply $x = -(z^* - z_{b,t})$. The CM and DM value functions for a buyer, $W^b(z_{b,t})$ and $V^b(z_{b,t})$, given her real balances $z_{b,t}$ obey the HJB equations formulated in the next lemma.

Lemma 4. *A representative buyer's value function is given by*

$$W^b(z_{b,t}) = z_{b,t} + W_0^b$$

$$rW_0^b = -z^* (r + \mu\pi) + \alpha \left[V^b(z^*) - W^b(z^*) \right] \tag{26}$$

Intuitively, buyers bear the cost of adjusting real balances to the optimal quantity z^* together with the cost of holding tokens without spending them originating from inflation and discounting. At rate α, buyers use their optimal amount of tokens to obtain a capital gain from DM trade. The DM value function $V^b(z^*)$ depends on the agreed bargaining terms between buyer and seller.

Sellers

Sellers enter the CM with real balances $z_{s,t}$ and a set of pending transactions waiting for validation on the blockchain and engage in DM according to a meeting rate α. To keep the model tractable, I assume that sellers are too busy to keep track of the number of the number of pending transactions they are waiting to receive and discount each of them independently. Hence they neglect the congestion effect caused by multiple pending transactions. As long meetings with buyers are rare enough at individual seller level, this assumption has negligible implications for the trade equilibrium. Sellers are passive except for selling their tokens, when available, and defining the terms of DM trade with buyers.

The value of a pending DM transaction is eroded by the depreciation caused by discounting and inflation until it is settled. For this reason, a transaction involving $z_{s,t}$ real tokens waiting for validation is discounted using a specific *validation discount factor* $\Omega \in [0, 1]$ that accounts for the effects of inflation and time discounting during the transaction settlement period. The resulting present value of a pending DM transaction is thus $z_{s,t}\Omega$.

The validation discount factor can be determined through the following observations. First, the discount factor that applies to a pending transaction waiting to be recorded in the next valid block is the product of a term resulting from temporal discounting, $\frac{\mu}{r+\mu}$,

continuous adjustment rule based on expected inflation.

(see Eq. (A.5)) and an inflation adjustment term, $1-\pi$, resulting in the expression

$$\frac{\mu}{r+\mu}(1-\pi) \tag{27}$$

Since a pending transaction is discounted by (27) each time the transaction waits for an additional valid block to be recorded, and given that the number of valid blocks posted until a transaction is recorded on the blockchain is distributed according to the geometric p.m.f. $d(n)$ from Eq. (22), the validation discount factor Ω follows from the next expectation:

$$\Omega \triangleq \mathbb{E}_n\left[\left(\frac{\mu}{r+\mu}(1-\pi)\right)\right]^{n+1} = \frac{(1-\pi)\mu\nu}{r+\mu\left(\nu+\pi(1-\nu)\right)} \qquad \text{with } \Omega_\pi<0,\ \Omega_{\pi\pi}>0,\ \Omega_{\pi,\nu}<0 \tag{28}$$

where the block inclusion probability ν is defined in Eq. (22). Now I am ready to present the representative seller's value function.

Lemma 5. *The value function of a seller at the time he records a pending transaction is given by*

$$W^s(\Omega z_{s,t}) = \Omega z_{s,t} + W_0^s \qquad \textit{with} \qquad rW_0^s = \alpha\left(V^s - W_0^s\right) \tag{29}$$

Where Ω is the validation discount factor determined in (28)

Intuitively, the seller's expected enjoyment from generic good consumption once his pending tokens are settled and immediately cashed-out to a CM amounts to $\mathbb{E}(x) = z_{s,t}\Omega$. In the meantime, the seller continues to trade at rate α with buyers.

In practice and in Chiu and Koeppl (2019), before delivering the special good to a buyer, sellers wait for the consensus chain to grow until the block recording her payment is deep enough inside it, so that the blocks built on top of it count as "confirmations" of the block's validity. Realistic terms of trade should also cover the *depth* of the valid block including the payment, where "depth" is intended as the distance between a block and the terminal block of the consensus chain. In BTC, the praxis is to wait for the consensus chain to grow by 6 blocks before accepting a payment, so that it takes one hour for a transaction to be considered safe. In Ethereum (ETH), sellers are advised to wait for 30 confirmations but block creation is considerably faster, so that it takes on average 6 minutes for a transaction to be safely considered as valid. Sellers accepting Bitcoin Cash (BCH) payments are suggested to wait for 15 confirmations so that transactions become valid, in expectation, after 2 hours and a half.

DM bargaining

When entering the DM, a buyer-seller pair b-s meets to agree on the terms of DM trade $(y, p(y))$ specified by an amount of special good units produced by s and a price paid

by b. Upon meeting, traders observe the current token prices and b reveals to s his real balances z. Since carrying liquidity is costly, b leaves the DM without tokens, so that $p(y) = z^*$ holds, i.e. the cash-in-advance constraint is binding. To facilitate exposition, in this section I let $z^* \equiv z$ and denote as $y(z)$ the amount of special good produced by the seller given his knowledge of the buyer's real balances.

Since digital wallets are programmed to charge a transaction fee τ, the seller receives only a part $z(1-\tau)$ of the value transferred by the buyer. The remaining $z\tau$ goes to the miner that records the transaction on the blockchain.

Right after setting the trade terms but before re-joining their respective CM's, the buyer enjoys utility $u(y(z))$ from consuming the special good and sends her tokens to the seller, while the seller spends a cost y to produce the special good and records a pending transaction of value $z(1-\tau)$. It follows that

$$V^b(z) = u\left(y(z)\right) + W_0^b \tag{30}$$

$$V^s = -y(z) + W^s\left(\Omega z(1-\tau)\right) \tag{31}$$

I determine the terms of trade using Kalai bargaining, according to which traders split the trade surplus in proportion to their bargaining power. To do so, notice that traders' outside options are $W^b(z)$ and W_0^s, hence their trading surpluses follow the equations

$$V^b(z) - W^b(z) = \underbrace{u\left(y(z)\right) + W_0^b - W^b(z)}_{=u\left(y(z)\right)-z} \quad \text{and} \quad V^s - W_0^s = \underbrace{-y(z) + W^s\left(\Omega z(1-\tau)\right) - W_0^s}_{=-y(z)+\Omega z(1-\tau)} \tag{32}$$

Thus, letting β denote buyers' bargaining weight, Kalai bargaining implies

$$u(y) - p(y) = \frac{\beta}{1-\beta}\left(-y + p(y)(1-\tau)\Omega\right) \quad \text{equivalent to} \quad p(y) = \frac{(1-\beta)u(y) + \beta y}{(1-\beta) + \beta(1-\tau)\Omega} \tag{33}$$

Plugging the resulting special good price back into the trade surplus expressions (32), we can see that traders share the (adjusted) total surplus in proportion to their bargaining power, so that the DM capital gain buyer and seller

$$V^b(z) - W^b(z) = \beta\,\frac{u(y(z))(1-\tau)\Omega + y(z)}{(1-\beta) + \beta(1-\tau)\Omega} \quad V^s - W_0^s = (1-\beta)\,\frac{u(y(z))(1-\tau)\Omega + y(z)}{(1-\beta) + \beta(1-\tau)\Omega}$$

Applying the formulae for the trade surpluses and special good price to these DM value functions, traders' DP equations now take explicitly into account the role of trade frictions, so that I can solve for buyers' optimal real balance portfolio z^*.

Lemma 6 (special good production and optimal token portfolio)**.** *The optimal amount of special good produced by sellers and the optimal token portfolio held by buyers (in real*

terms) are determined as follows:

$$y^* : \frac{1}{\alpha}(r+\mu\pi) \underbrace{\leq}_{=\text{ if } y^*>0} \frac{u'(y^*)}{p'(y^*)} - 1, \quad z^* = p(y^*) \tag{34}$$

The optimal token portfolio is determined by equating costs and benefits of carrying tokens. The cost of increasing marginally real balances is the sum of the marginal discounting r and inflation cost $\mu\pi$ paid to maintain the optimal amount of real balances while keeping-up with inflation. Both costs are incurred for a period of time of expected length $1/\alpha$. The benefit of holding marginally more liquidity (tokens in this case) is expressed by the right-side of inequality (34) and measures the sensitivity of the DM capital gain with respect to real balances. The LW literature defines this marginal effect as the "liquidity premium" (see Choi and Rocheteau (2020b) or Lagos et al. (2014) for some examples of usage).

As previously anticipated, for a positive inflation rate buyers do not carry more tokens than those needed in the DM. The opposite happens for a (sufficiently) deflationary cryptocurrency whose tokens gain value over time. This feature makes a deflationary cryptocurrency more suited to be used as a safe-heaven asset rather than as a means of payment.

An explicit formula for y^* is easily obtained from Eqs. (33) and (34) under the assumption that buyers have full bargaining power ($\beta = 1$). Making explicit the utility function (1), we have

$$y^* = y(z^*) = \frac{\alpha(1-\tau)\Omega}{r+\alpha+\mu\pi} - \frac{1}{\eta} \tag{35}$$

$$z^* = \frac{\alpha}{r+\alpha+\mu\pi} - \frac{1}{\eta(1-\tau)\Omega} \tag{36}$$

Buyers' desired level of special good consumption y^* is decreasing in the transaction fee rate and congestion (lower Ω) owing to worse contractual terms. Notice that a large enough value of η ensures that $y^* > 0$.

5 Monetary equilibrium

In this section, I combine the partial equilibrium models of Section 4 and determine the monetary (general) equilibrium of the economy.

Equation (33) can be used as an asset-pricing identity by decomposing real balances into a number of tokens held and tokens' price: $p(y^*) = z^* = \phi_{i,t} a_{b,t}$, where i is the index of the CM in which b operates. CM prices follow from aggregating the condition (33)

over the CM's buyer population.

$$\phi_{i,t} = \frac{p(y^*)}{A_{i,t}} B_i = \text{ for } i = 1, 2$$

The Market clearing condition (2) together with the stationary property (3) and the inflation schedule (9) pin-down the dynamic evolution of a DM price for a given initial amount of tokens in circulation A_{i,t_0} $\forall i$ as follows. Letting b_t indicate the number of valid blocks produced by time t,

$$\begin{aligned} \mathbb{E}\left(\phi_{i,t}\right) &= \frac{B}{2}\frac{p(y^*)}{A_{i,t_0}}\frac{\mathbb{E}\left(\phi_{i,t} \mid \phi_{i,t_0}\right)}{\phi_{i,t_0}} \quad \text{with } \frac{\mathbb{E}\left(\phi_{i,t} \mid \phi_{i,t_0}\right)}{\phi_{i,t_0}} = \mathbb{E}\left[(1-\pi)^{b_t - b_{t_0}}\right] = e^{-\pi\mu(t-t_0)} \\ &= \frac{B}{2}\frac{p(y^*)}{A_{i,t_0}} e^{-\pi\mu(t-t_0)} \end{aligned} \tag{37}$$

A complete derivation of the previous formula is contained in Appendix B. Expected prices fall exponentially at the rate of seigniorage and depend positively on tokens' utilization through the special good price.

The general monetary equilibrium of the economy puts together all elements determined so far and closes the model.

Definition 3 (Cryptocurrency Equilibrium)**.** *Given the design parameters* (μ, π, τ) *and initial tokens in circulation* A_{i,t_0} *for* $i = 1, 2$*, a cryptocurrency (monetary) equilibrium with permanent mining is a collection of value functions* (W_0^m, W_0^b, W_0^s)*, (23,26,29) optimal controls* (σ^*, z^*, y^*) *(16, 34, 35), prices* $\left(p(y), \left(\phi_{i,t}\right)_{i=1,2}\right)$ *(33,37) and distributions* $(g(\cdot), d(\cdot))$ *(21,22) such that (i) all agents make optimal decisions (ii) market clearing (2) holds in each CM (iii) the validation discount factor applied to DM transactions is determined by equation (28). (iv) miners play a permanent mining equilibrium and entry the economy according to expression (25).*

This equilibrium is a standard forward-looking monetary equilibrium with policy parameters linked to the blockchain's internal functioning. Monetary policy is determined by the amount of tokens created by coinbase transactions and the block creation rate. Record-keeping is performed by miners, provided that they have the incentive to do so.

The existence of a cryptocurrency equilibrium requires a contained level of congestion. If congestion gets out of control, settlement times become huge, so that sellers charge a prohibitive price for the special good and no buyer can benefit from trading in the DM market, the only reason for them to hold tokens in this model. In the extreme case in which miners refuse to fill blocks, congestion becomes infinite. It is therefore essential that the protocol is designed in such a way to incentivize mining.

6 Optimal cryptocurrency design

In this section, I take a normative standpoint and study the optimal design of a cryptocurrency. Specifically, I study the problem of a blockchain protocol designer who sets inflation, block rate, and transaction fees to elicit a secure level of miner participation and incentivize miners to fill blocks. The designer, or social planner (SP), can be thought of as a software developer designing a modification of the Bitcoin source code.

In a standard optimal taxation problem, the government can dictate the supply of public goods. In blockchain design instead, miners' behavior is guided by their incentives, so the protocol sets the policy instruments (μ, π, τ) to induce miners in providing a level of public goods $(M, k(Q))$. Miner participation M raises blockchain security, a pure public good, but also creates a welfare loss caused by the PoW energy costs.[23] On the other hand, processing capacity (or mining throughput) resulting from miners' block size strategies $k(Q)$ is a common-pool good subject to congestion.

The planner's problem can be formalized as the maximization of agents' aggregate utility subject to mining and trade incentive compatibility constraints. Maintaining the assumption that buyers have full bargaining power simplifies the welfare expression since $W_0^{s,0} = 0$. Furthermore, the free-entry condition is such that miner participation is the highest admissible value that provides miners a non-negative surplus. If M where continuous, free-entry would set mining rents to zero. However, under the assumption that M is discrete, miners can still earn a positive rent due to a mere integer rounding. So, for simplicity, I will ignore the rounding issue and treat miners as if they earn no surplus, i.e. setting $W_0^{m,0} = 0$. As a result of these simplifications, the planner simply maximizes per-buyer surplus.

$$W^{SP} = \max_{\mu,\pi,\tau} W_0^b, \qquad W_0^b = \frac{\alpha}{r}\left(u\left[y(z^*)\right]\right) - z^*\left(1 + \frac{\mu\pi}{r}\right) \tag{38}$$

$$\text{subject to } M = \underline{M} \text{ and optimal } (\sigma^*, y^*, z^*)$$

Notice that eliciting miner participation beyond $\underline{M}$ creates only a dead-weight loss, so letting miners only up to the secure level of participation is optimal in any design. Also, since the mixed-strategy mining MPE is not a reasonable prediction of mining behaviour, the planner has to preclude miner inactivity at any point in time to make sure that miners perform their record-keeping task when there are pending transactions and continue building the blockchain keep it secure when the mem-pool is empty. In other words, the planner implements a permanent mining equilibrium.

[23] Current estimates from https://digiconomist.net/bitcoin-energy-consumption indicate that Bitcoin annual energy consumption accounts for approximately 0.21% of the world's total, producing a carbon footprint comparable to that of a small country - around 33 CO2 megatons. Several protocol proposals aim to address the sustainability issue associated with Bitcoin PoW.

6.1 Contribution to the fees-versus-seigniorage debate

In Chiu and Koeppl (2019), an optimally designed cryptocurrency rewards miners only with seigniorage. CK's result follows from the observation that inflation is paid on a larger "tax base" than transaction fees, so the designer can guarantee miners a given amount revenues by charging commodity traders at a lower rate than one implied by a design that also uses fees. However this argument ignores the effects of inflation on the rate of per-block transactions that miners record and hence on the speed at which payments are processed.

In particular, with endogenous block size, raising inflation reduces the size of blocks formed by miners, which in turn produces the welfare-reducing effect of making settlement times of pending transactions longer. In the extreme case in which miners produce only empty blocks, settlement times are infinite, so the cryptocurrency infrastructure cannot sustain a monetary equilibrium.

In this model, a pure seigniorage reward causes this scenario to occur. Nevertheless, the protocol can avoid such situation by setting a lower bound on fees so to ensure that miners take charge of their role of record-keepers. The safest scenario that the protocol can enforce is the one in which miners have a dominant strategy to play a permanent (maximal) mining equilibrium. In other words, each miner finds optimal to fill blocks regardless what other miners do. If this is the case, a monetary equilibrium is implementable in dominant mining strategies.

Definition 4. *A policy* (μ, π, τ) *implements a mining equilibrium* $\boldsymbol{\sigma}(\mu, \pi, \tau)$ *in dominant strategies if and only if*

$$\mathbb{E}_{\sigma(\mu,\pi,\tau),\boldsymbol{\sigma}_{-\boldsymbol{m}}}\left[R\left(k_m(Q)\right) \mid Q\right] \geq \mathbb{E}_{\sigma'_m,\boldsymbol{\sigma}'_{-\boldsymbol{m}}}\left[R\left(k_m(Q)\right) \mid Q\right], \quad \forall \sigma'_m, \boldsymbol{\sigma}_{-m}, Q$$

Dominant strategy implementation of maximal mining requires the fee-to-seigniorage ratio to satisfy Proposition 1-(i). This combined with the activity condition (20) and security condition $M \equiv \lceil M^* \rceil = \underline{M}$, with equilibrium miner entry given by (25). These constitute the constraints that the planner has to satisfy when choosing policy parameters optimally. To summarize, the planner maximizes (38) subject to

$$\begin{aligned}
\frac{\tau}{\pi} &\geq \frac{\mu B}{2\theta} && \text{Record-keeping constraint} && \text{(KEP)} \\
3 &> \frac{Bz^*(\pi,\tau)(\mu\pi + \alpha\tau)}{\psi + rF} \geq 2 && \text{Security constraint} && \text{(SEC)} \\
\pi &\geq \frac{2\psi}{\mu B} && \text{Activity constraint} && \text{(ACT)}
\end{aligned}$$

The general design problem is complicated and beyond the scope of the current version of this paper that only analyzes record-keeping incentives with a two-miner population.

Yet, we can already provide a simple optimal design with the analysis developed so far. In particular, notice that if a secure participation $\underline{M} = 2$ can be achieved with the lowest admissible value (π^*, μ^*) implied by the above constraints, that is an optimal design. Even though this is a simplistic approach to the general problem, it is already instructive as it shows an example where the optimal level of fees is positive. The following proposition presents a simple closed-form expression for such minimal feasible rates of fees and seigniorage as well the condition under which miner secure entry is achieved and hence the design is optimal.

Proposition 2. *For $\underline{M} = 2$, the lowest rates (π, τ) that can implement a monetary equilibrium in dominant mining strategy $(\sigma = 1)$ are*

$$\pi = \frac{2\psi}{\mu B} \qquad \tau = \frac{\psi}{\theta} \tag{39}$$

For fixed μ, these rates constitute an optimal design if the security constraint is (SEC) is satisfied at those values.

Notice that both seigniorage and transaction fee rates are increasing in the energy cost of mining, but the fee rate decreases in the block propagation rate, which raises miner chances to record blocks and cash-in the fees associated to them, while the inflation rate decreases in the size of the buyer population at which cryptocurrency deposits will be charged.

6.2 Discussion

Proposition 2 assumes that the security requirement $\underline{M}$ is independent of the policy instruments mix. In CK instead, higher fees increase the secure (honest) miners' participation requirement because, by reversing transactions with DS attacks, fraudulent miners - that in CK are also buyers - reverse to themselves the value of transaction fees as well. However, in practice, transaction fees are small relative to the capital gain that makes a fraud worthwhile and have mild effects on miners' incentives to misbehave. For this reason, it is realistic to consider as negligible the impact of τ on $\underline{M}$.

Finally, an alternative but less robust argument for justifying reducing seigniorage in favour of transaction fees is based on the "hot potato effect" of inflation. According to this argument, higher seigniorage (and inflation), raises the velocity of money, i.e. induces traders to spend their tokens at a faster rate, creating a negative congestion externality. Analyzing this argument requires modelling buyers' endogenous intensity of search for sellers, possibly adapting Ennis (2009) model to continuous time cryptocurrency economy studied so far.

7 Conclusion

I presented a model that describes the plurality of interactions involved in a cryptocurrency economy. Miners play the essential role of record-keepers by recording blocks of transactions on their copies of the cryptocurrency blockchain. They also contribute to the blockchain security and resolve inconsistencies among their ledger copies by following the Longest-Chain-Rule, indicating them a unique branch of the ledger to follow.

Sellers receive transactions from buyers only after they are recorded by miners on the blockchain. As a result, transaction settlement is stochastic and depends on miners' block size strategy. Since larger blocks imply a short transaction settlement period, traders are always better-off if miners choose to create large blocks; however, miners do not always benefit from doing so. Indeed, miners increase the size of their blocks only if the higher transaction fees compensate for the higher risk that their blocks become stale due to their slow transmission time caused by having a large dimension.

Small blocks lead to a higher load of pending transactions on the blockchain and worsen the terms of cryptocurrency trade. In the extreme case in which miners only create empty blocks, transactions never get processed, and a monetary equilibrium in which cryptocurrency trade takes place is not plausible. A clever blockchain design can avoid this scenario by setting high enough transaction fees relative to seigniorage, thereby providing miners with the incentive to fill blocks.

The analysis developed in this paper studied in detail the basic mining trade-off involving block reward and the risk of blocks becoming stale caused by slow block transmission. Further research could extend the model developed in this paper by introducing verification times and SPV mining. In practice, each time a miner receives a block he has to spend a *verification time* to check the block's validity. Afterwards, if the verification has a positive outcome, he updates his ledger and mem-pool with the information contained in the verified block, whereas in the contrary case - e.g. if the block contains double-spent transactions or an invalid PoW - he forks-it out in a stale branch. A miner cannot safely mine new non-empty blocks while preforming a verification, as they can cause a double-spending with the transactions included in the block under verification, but faces no risk in mining empty blocks while verification is still incomplete. The practice of creating empty blocks skipping full verification is known as Simplified Payment Verification (SPV) mining. The practice has the positive effect of precluding mining-gaps and thus rises mining revenues and in turn the level of blockchain security against malicious attacks. These mining incentives are particularly important when miners' mem-pools are empty ($Q = 0$). Nevertheless, SPV mining is a form of free-riding when miners' mem-pools are non-empty ($Q > 0$) and allows record-keeping errors to remain unnoticed for long, amplifying their detrimental effects when finally revealed.

Finally, by letting cryptocurrency prices vary across CM's, the model can be used to

address traders' incentives to engage in speculation.

References

Abadi, J. and Brunnermeier, M. (2018). Blockchain economics. Technical report, National Bureau of Economic Research.

Athey, S., Parashkevov, I., Sarukkai, V., and Xia, J. (2016). Bitcoin pricing, adoption, and usage: Theory and evidence.

Biais, B., Bisiere, C., Bouvard, M., and Casamatta, C. (2019). The blockchain folk theorem. *The Review of Financial Studies*, 32(5):1662–1715.

Budish, E. (2018). The economic limits of bitcoin and the blockchain. Technical report, National Bureau of Economic Research.

Carlsten, M., Kalodner, H., Weinberg, S. M., and Narayanan, A. (2016). On the instability of bitcoin without the block reward. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 154–167.

Chiu, J. and Koeppl, T. (2019). The Economics of Cryptocurrencies—Bitcoin and Beyond. Staff Working Papers 19-40, Bank of Canada.

Choi, M. and Rocheteau, G. (2020a). Money mining and price dynamics. *Available at SSRN 3336367*.

Choi, M. and Rocheteau, G. (2020b). More on money mining and price dynamics: Competing and divisible currencies. *Available at SSRN*.

Choi, M. and Rocheteau, G. (2020c). New monetarism in continuous time: Methods and applications. *Available at SSRN 3435889*.

Cong, L. W., He, Z., and Li, J. (2019). Decentralized mining in centralized pools. Technical report, National Bureau of Economic Research.

Decker, C. and Wattenhofer, R. (2013). Information propagation in the bitcoin network. In *IEEE P2P 2013 Proceedings*, pages 1–10. IEEE.

Easley, D., O'Hara, M., and Basu, S. (2019). From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics*.

Ennis, H. M. (2009). Avoiding the inflation tax. *International Economic Review*, 50(2):607–625.

Eyal, I. and Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security*, pages 436–454. Springer.

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

Grunspan, C. and Pérez-Marco, R. (2018). Double spend races. *International Journal of Theoretical and Applied Finance*, 21(08):1850053.

Houy, N. (2016). The bitcoin mining game. *Ledger*, 1:53–68.

Huberman, G., Leshno, J., and Moallemi, C. C. (2019). An economic analysis of the bitcoin payment system. *Columbia Business School Research Paper*, (17-92).

Kroll, J. A., Davey, I. C., and Felten, E. W. (2013). The economics of bitcoin mining, or bitcoin in the presence of adversaries. In *Proceedings of WEIS*, volume 2013, page 11.

Lagos, R., Rocheteau, G., and Wright, R. (2014). The art of monetary theory: A new monetarist perspective. *forthcoming, Journal of Economic Literature*.

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

Leshno, J. D. and Strack, P. (2019). Bitcoin: An axiomatic approach and an impossibility theorem. *American Economic Review: Insights*.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Cryptography Mailing list at https://metzdowd.com*.

Neudecker, T. and Hartenstein, H. (2019). Short paper: An empirical analysis of blockchain forks in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 84–92. Springer.

Pinzón, C. and Rocha, C. (2016). Double-spend attack models with time advantange for bitcoin. *Electronic Notes in Theoretical Computer Science*, 329:79–103.

Prat, J. and Walter, B. (2018). An equilibrium model of the market for bitcoin mining.

Rizun, P. R. (2015). A transaction fee market exists without a block size limit. *Block Size Limit Debate Working Paper*.

Rosenfeld, M. (2014). Analysis of hashrate-based double spending. *arXiv preprint arXiv:1402.2009*.

Rosu, I. and Saleh, F. (2019). Evolution of shares in a proof-of-stake cryptocurrency. *Available at SSRN 3377136*.

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., and Mohaisen, A. (2019). Exploring the attack surface of blockchain: A systematic overview. *arXiv preprint arXiv:1904.03487*.

Saleh, F. (2020). Blockchain without waste: Proof-of-stake. *Available at SSRN 3183935*.

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

Appendix A Additional derivations

A.1 Distributions of mem-pools' size and validation times

Mem-pools

The steady state distribution of the mem-pool balances expected in-flows and out-flows of transactions. For $Q_t > 0$, miners receive transactions at rate $\lambda \equiv \alpha B$ and process transactions at rate $\sigma\mu$. If $Q_t = 0$ instead, miners have no transaction to process. Let $\dot{Q}_t \triangleq \partial Q_t/\partial t$. We have

$$\dot{g}(0) = \mu\sigma g(1) - \lambda g(0) \tag{A.1}$$

$$\dot{g}(Q) = \lambda g(Q-1) + \mu\sigma g(Q+1) - (\lambda + \mu\sigma)\, g(Q) \qquad \text{for } Q > 0 \tag{A.2}$$

$$\text{with } \textstyle\sum_{Q=0}^{\infty} g(Q) = 1 \tag{A.3}$$

Setting $\dot{g}(Q) = 0\ \forall Q$ yields $g(Q) = \rho g(Q-1)$, where $\rho = \lambda/\sigma\mu$ denotes the load factor, implying $g(Q) = \rho^Q g(0)$ for all $Q \geq 0$. Applying the normalization (A.3) we obtain the stationary probability of the mem-pool being empty,

$$\textstyle\sum_{Q=0}^{\infty} \rho^Q g(0) = \dfrac{g(0)}{1-\rho}, \text{ so, } g(0) = 1 - \rho$$

Now we can see that the mem-pool distribution is geometric with p.m.f. $g(Q) = (1-\rho)\rho^Q$ ■

Remark: In a permanent mining equilibrium ($\sigma = 1$) the mining game defined in Section 4.1 switches across mem-pool states according to the following transition rate

matrix

$$\begin{array}{c} \\ (Q,H),\ Q=0 \\ (Q,H),\ Q>0 \end{array} \begin{array}{c} \begin{array}{cccc} (Q,H) & (Q+1,H) & (Q,H+1) & (Q-1,H+1) \end{array} \\ \begin{bmatrix} 1-\lambda-\mu & \lambda & \mu & 0 \\ 1-\lambda-\mu & \lambda & 0 & \mu \end{bmatrix} \end{array}$$

Validation time

Suppose miners form blocks picking transactions uniformly at random from their mempools and each seller has at most one pending transaction. The probability that a pending transaction directed to seller s is recorded in a block is $1/(1+Q_{-s})$, where Q_{-s} is the number of pending transactions not yet recorded and directed towards other sellers. Since seller s takes into account that Q_{-s} is geometrically distributed with p.m.f. $g(Q)$ (from Eq. (21)), she computes the probability that her transaction will be included in the next block using the following formula:

$$\sum_{Q_{-s}=0}^{\infty} g(Q_{-s})\frac{1}{1+Q_{-s}} = (1-\rho)\sum_{Q_{-s}=0}^{\infty}\frac{\rho^{Q_{-s}}}{1+Q_{-s}} = \frac{1-\rho}{\rho}\left(\sum_{Q=1}^{\infty}\frac{\rho^{Q}}{Q}\right) = \frac{1-\rho}{\rho}\ln(1-\rho)^{-1} \tag{A.4}$$

where the last equality follows from the Maclaurin expansion of $\ln(1-\rho)^{-1}$. Since miners fill blocks with probability σ, it follows that a transaction's validation time in block units is geometrically distributed with p.m.f. $d(n) = (1-\nu)^{n-1}\nu$, in which the block inclusion parameter ν satisfies $\nu = \sigma\frac{1-\rho}{\rho}\ln(1-\rho)^{-1}$ ■

A.2 Properties of agents' value functions

To follow the main proofs in Appendix B and part of the analysis contained in the main body of the paper, it is worth to keep in mind some properties of value functions driven by an underlying Poisson process and Poisson processes themselves.

Exponential random variables:

Let $\{T_j\}_{j\in\{1,2,\ldots,J\}}$ denote a collection of exponential random variables with with rates $\{\alpha_j\}_{j\in\{1,2,\ldots,J\}}$. Their minimum $T = \min\{T_j\}_{j\in\{1,2,\ldots,J\}}$ is again exponentially distributed with rate $\alpha = \sum_{j\in\{1,2,\ldots,J\}}\alpha_j$. Moreover, since the Laplace-Stieltjes transform of the exponential random variable T_j is given by $\mathbb{E}\left(e^{-rT_j}\right) = \frac{\alpha_j}{r+\alpha_j}$, so we also have that

$$\mathbb{E}\left(e^{-rT}\right) = \alpha/(r+\alpha) \tag{A.5}$$

Stochastic upper integration limit:

Let T_j denote an exponential RV with rate α_j. The following identity holds:

$$\mathbb{E}_{T_j}\left(\int_0^{T_j} e^{-rt} f(t)\,\mathrm{d}t\right) = \int_0^{\infty} e^{-(r+\alpha_j)t} f(t)\,\mathrm{d}t \tag{A.6}$$

To see this, integrate the left-hand side of Eq. (A.6) by parts, setting $v(T_j) = -e^{-\alpha_j T_j}$ and $u'(T_j) = e^{-rT_j} h_{T_j}$ to obtain

$$\begin{aligned}\mathbb{E}_{T_j}\left(\int_0^{T_j} e^{-rt} f(t)\,\mathrm{d}t\right) &= \int_0^{\infty} \alpha_j e^{-\alpha_j T_j}\left(\int_0^{T_j} e^{-rt} f(t)\,\mathrm{d}t\right)\mathrm{d}T_j \\ = \int_0^{\infty} v'(T_j)u(T_j)\,\mathrm{d}T_j &= \underbrace{\Big[v(T_j)u(T_j)\Big]_0^{\infty}}_{=0} - \int_0^{\infty} v(T_j)u'(T_j)\,\mathrm{d}T_j \\ &= \int_0^{\infty} e^{-(r+\alpha_j)T_j} f(T_j)\,\mathrm{d}T_j \equiv \int_0^{\infty} e^{-(r+\alpha_j)t} f(t)\,\mathrm{d}t \quad \blacksquare\end{aligned}$$

Switching Poisson states:

Suppose a value function W^0 can switch from state 0 to states $j \in \{1, 2, \ldots, J\}$ at a Poisson rates $\alpha_{0j} \equiv \alpha_j$. Then, as we saw earlier in this section, the switching-time T from state 0 to a next generic state is exponentially distributed with cumulative transition rate α and the probability that the value function will enter a given state j next is α_j/α. Therefore,

$$W^0 = \mathbb{E}_{T,j}\left(e^{-rT} W^j\right) = \frac{\alpha}{r+\alpha}\left(\sum_{j\in\{1,2,\ldots,J\}} W^j \frac{\alpha_j}{\alpha}\right) = \frac{1}{r+\alpha}\sum_{j\in\{1,2,\ldots,J\}} \alpha_j W^j$$

It follows that

$$rW^0 = \sum_{j\in\{1,2,\ldots,J\}} \alpha_j\left(W^j - W^0\right) \quad \blacksquare \tag{A.7}$$

Appendix B Omitted proofs

Proof of Lemma 1. If $\gamma_{H+1,m} + \epsilon_{H+1,m} < \min_{m'}\left\{\gamma_{H+1,m'} + \epsilon_{H+1,m'}\right\}$, miner m's transmission time is fast enough to let him establish the next reference predecessor block and collects the block reward. If not, m's block gets forked-out by all other miners. For now, let $\gamma_{H+1,m} \equiv \gamma_m$ and $\epsilon_{H+1,m} \equiv \epsilon_m$ for a given $m \in \mathcal{M}$. The probability $\tilde{P}_{M-1}(T; \boldsymbol{\sigma}_{-\boldsymbol{m}} = \boldsymbol{\sigma})$ that a block with update time $T_{H+1,m} \equiv T$ is faster than the contemporaneous $M-1$ blocks, evaluated using the belief $\boldsymbol{\sigma}_{-\boldsymbol{m}} = \boldsymbol{\sigma}$ on other miners' block strategies, satisfies

the following relationships

$$\tilde{P}_{M-1}(T;\boldsymbol{\sigma_{-m}}=\boldsymbol{\sigma}) = \mathbb{P}\left(\min_{m'}\{\gamma_{m'}+\epsilon_{m'}\}>T\right) = \left(1-F_{\gamma_{m'}+\epsilon_{m'}}(T)\right)^{M-1}$$
$$= \left[e^{-T(\mu/M)} + \sigma\frac{\mu/M}{\theta-(\mu/M)}\left(e^{-T(\mu/M)}-e^{-T\theta}\right)\right]^{M-1} \tag{B.8}$$

The unconditional belief of successful mining $P(\sigma_m, \boldsymbol{\sigma_{-m}})$ is obtained from expression (B.8) by integrating-out the marginal density of T, so that

$$P(\sigma_m;\boldsymbol{\sigma_{-m}}) = \int_0^\infty \tilde{P}(t,\boldsymbol{\sigma_{-m}}) f_{\gamma_m+\epsilon_m}(t)\,\mathrm{d}t \tag{B.9}$$

Now, integrating Eq. (B.9) by parts,

$$\int_0^\infty P_1(t)^{M-1} f(t)\,\mathrm{d}t = \left[P_1(t)^{M-1}\left(1-P_1(t)\right)\right]_{t=0}^{t\to\infty} + (M-1)\int_0^\infty P_1(t)^{M-2}\left(1-P_1(t)\right) f(t)\,\mathrm{d}t$$
$$= \underbrace{\left[P_1(t)^{M-1} - P_1(t)^M\right]_{t=0}^{t\to\infty}}_{=0} + (M-1)\int_0^\infty P_1(t)^{M-2} f(t) - P_1(t)^{M-1} f(t)\,\mathrm{d}t$$
$$\int_0^\infty P_1(t)^{M-1} f(t)\,\mathrm{d}t = (M-1)\left[\int_0^\infty P_1(t)^{M-2} f(t)\,\mathrm{d}t\right] - (M-1)\left[\int_0^\infty P_1(t)^{M-1} f(t)\,\mathrm{d}t\right]$$

Collecting the identical integrals,

$$\int_0^\infty P_1(t)^{M-1} f(t)\,\mathrm{d}t = \frac{M-1}{M}\left[\int_0^\infty P_1(t)^{M-2} f(t)\,\mathrm{d}t\right] \tag{B.10}$$

Expression (12) follows immediately from Eq. (B.10) proceeding by induction on M with base step $M=2$ ■

Proof of Lemma 2. From Eq. (B.9) the probability we are looking for is the result of the following integral

$$P(\sigma_m,\sigma_{-m}) = \int_0^\infty \left[e^{-T\frac{\mu}{2}} + \sigma_{-m}\frac{\mu}{2\theta-\mu}\left(e^{-T\frac{\mu}{2}} - e^{-T\theta}\right)\right]$$
$$\times\left[\sigma_m\frac{\theta\mu}{2\theta-\mu}\left(e^{-T\frac{\mu}{2}}-e^{-T\theta}\right) + \frac{\mu}{2}(1-\sigma_m)e^{-T\frac{\mu}{2}}\right]\mathrm{d}T \tag{B.11}$$

Expand the product in the previous expression and integrate each part separately.

We have that

$$\left(\sigma_m \frac{\theta\mu}{2\theta-\mu}\right)\int_0^\infty e^{-T\frac{\mu}{2}}\left(e^{-T\frac{\mu}{2}}-e^{-T\theta}\right)\mathrm{d}T$$
$$=\left(\sigma_m \frac{\theta\mu}{2\theta-\mu}\right)\frac{2\theta-\mu}{\mu(2\theta+\mu)}$$
$$=\frac{\sigma_m\theta}{2\theta+\mu}$$

$$\frac{\mu}{2}(1-\sigma_m)\int_0^\infty e^{-T\mu}\,\mathrm{d}T=\frac{1-\sigma_m}{2}$$

$$\left(\sigma_{-m}(1-\sigma_m)\frac{\mu^2}{2(2\theta-\mu)}\right)\int_0^\infty e^{-T\frac{\mu}{2}}\left(e^{-T\frac{\mu}{2}}-e^{-T\theta}\right)$$
$$=\left(\sigma_{-m}(1-\sigma_m)\frac{\mu^2}{2(2\theta-\mu)}\right)\frac{2\theta-\mu}{\mu(2\theta+\mu)}$$
$$=\frac{(1-\sigma_m)\sigma_{-m}\mu}{2(2\theta+\mu)}$$

$$\left(\sigma_{-m}\sigma_m\frac{\mu^2\theta}{(2\theta-\mu)^2}\right)\int_0^\infty\left(e^{-T\frac{\mu}{2}}-e^{-T\theta}\right)^2\mathrm{d}T$$
$$=\left(\sigma_{-m}\sigma_m\frac{\mu^2\theta}{(2\theta-\mu)^2}\right)\frac{(\theta-\mu/2)^2}{\theta\mu(\theta+\mu/2)}$$
$$=\frac{\sigma_{-m}\sigma_m\mu}{2(2\theta+\mu)}$$

Summing up the four factors we obtain

$$P(\sigma_m,\sigma_{-m})=\frac{2\sigma_m\theta+2\theta(1-\sigma_m)+\mu(1-\sigma_m+\sigma_{-m}(1-\sigma_m+\sigma_m))}{4\theta+2\mu}=\frac{2\theta+(1-\sigma_m+\sigma_{-m})\mu}{4\theta+2\mu}$$

This probability is identical to the one displayed in Eq. (13). ■

Proof of Lemma 3. Since miners instantly sell their block rewards of value z_m and obtain linear utility from consuming the corresponding amount of numeraire good, we have that $W_M^m(z_m)=z_m+W_{0,M}^m$.

The component $W_{0,M}^m$ of the value function can be obtained by summing-up the expected payoffs obtained at each mining round, discounted at present value. Since miners consider the length of a mining round $T_{H+1}^*-T_H^*$ as exponentially distributed with rate μ, property (A.6) yields

$$\mathbb{E}\left[\psi\int_0^{T_{H+1}^*-T_H^*}e^{-rt}\,\mathrm{d}t\,\middle|\,T_H^*\right]=\psi\int_0^\infty e^{-(r+\mu)t}\,\mathrm{d}t=\frac{\psi}{r+\mu}\tag{B.12}$$

On the other hand, the present value of the block reward, discounted for the expected length of a mining round is obtained by computing

$$\mathbb{E}\left(e^{-r(T^*_{H+1}-T^*_H)}R(Q_{H+1})\right) \underbrace{=}_{g_t(Q_t)=g(Q_t)\forall t} \mathbb{E}\left(e^{-r(T^*_{H+1}-T^*_H)}R(Q)\right) \underbrace{=}_{\text{from (A.5)}} \frac{\mu}{r+\mu}\mathbb{E}\left[R(Q)\right] \tag{B.13}$$

with

$$\begin{aligned}\mathbb{E}\left[R(Q)\right] &= g(0)\left[R(0)P_{M-1}(0,0)\right] + (1-g(0))\left[\sigma R(1)P(1,\sigma) + (1-\sigma)R(0)P_{M-1}(0,\sigma)\right] \\ &= R(0)\Big((1-\rho)P_{M'}(0,0) + \rho(1-\sigma)P_{M'}(0,\sigma)\Big) + R(1)\sigma P_{M'}(1,\sigma)\end{aligned} \tag{B.14}$$

The expression resulting by the combination of Eqs. (B.12) to (B.14) is

$$\begin{aligned}W_0^m &= \frac{\mu\left(\mathbb{E}\left[R(Q)\right] + W_0^m\right) - \psi}{r+\mu} \\ \text{so that } W_0^m &= \frac{\mu\mathbb{E}\left[R(Q)\right] - \psi}{r}\end{aligned} \tag{B.15}$$

To obtain miners' value function (23), subtract from Eq. (B.15) the value of the initial investment in the mining node F and add real balances ■

Proof of Lemma 4. Using property (A.7), we have

$$\begin{aligned}W^b(z) &= -(z^*-z) + \frac{\mu W^b(z^*(1-\pi)) + \alpha V^b(z^*)}{r+\mu+\alpha} \\ (r+\mu+\alpha)W^b(z) &= -(z^*-z)(r+\mu+\alpha) + \mu W^b(z^*(1-\pi)) + \alpha V^b(z^*) \\ rW^b(z) &= -(z^*-z)(r+\mu+\alpha) + \mu\left[W^b\left(z^*(1-\pi)\right) - W^b(z)\right] + \alpha\left[V^b(z^*) - W^b(z)\right] \\ rW^b(z) &= -(z^*-z)r + \mu\left[W^b\left(z^*(1-\pi)\right) - W^b(z^*)\right] + \alpha\left[V^b(z^*) - W^b(z^*)\right] \\ rW^b(z) &= -(z^*-z)r - \mu\pi z^* + \alpha\left[V^b(z^*) - W^b(z^*)\right]\end{aligned}$$

Expression (26) follows by setting $z=0$ ■

Proof of Lemma 5. Immediate from property (A.7) and the derivations in Appendix A.1 ■

Appendix C Notation

t	time index	α	DM meeting rate
b, B; s, S; m, M	agents' index and population	x	generic good consumption
y	special good consumption	$u(\cdot)$	special good utility
$a_{i,t}$	nominal balances, $i \in \{b, s, m\}$	$z_{i,t}$	real balances, $i \in \{b, s, m\}$
B_{i}, S_{i}	subscribed buyers and sellers	$A^D_{i,t}$, $A^S_{i,t}$, $A_{i,t}$, A_t	token demand and supply
$Z_{i,t}$, Z_t	real balances in CM_i	$\phi_{i,t}$, ϕ_t	tokens' price in CM_i
$R(k)$	block reward for block size k	π	seigniorage rate
τ	proportional fee rate	h, H	block and blockchain height
$T_{h,m}$	publication time of block (h, m)	T^*_H	publication time of ref. block
μ, μ_m	block creation and mining PoW rate	$k_m(Q)$	block size Markov strategy
λ	transaction request rate	r	discount rate
$\underline{M}$	safe miners' participation	f, $\tilde{f}$	actual and approx. density
θ	block transmission rate	F, ψ	up-front and flow mining cost
$\mathcal{M}$	set of miners' labels	$\mathcal{U}_i$	life-time utility of agent
$\gamma_{h,m}$	PoW solution time	$\epsilon_{h,m}$	transmission lag
σ_m	prob. of filling a block	$p(y)$	price of the special good
Q	miners' mem-pools size	n	block number
$g(\cdot)$	p.m.f. of mempool size	$d(\cdot)$	p.m.f. of validation time
ρ	load factor	ν	probability of validation
β	buyers bargaining weight	Ω	validation discount rate

Appendix D Glossary

Altcoins	Cryptocurrencies originated from forks of BTC
Bitcoin (BTC)	The original implementation of the Bitcoin blockchain
bitcoin	A Bitcoin token
blockchain	A copy of a distributed ledger
coinbase transaction	The transaction awarding a miner with new tokens
fork	A bifurcation of the blockchain
genesis block	The first block of a blockchain
hash	A code resulting from an encryption
hashpower	Time rate of hash codes produced by the mining node
height (block)	Distance between a generic block and the genesis block
longest chain rule (LCR)	The consensus formation rule employed by most PoW blockchains
mining node	A computer endowed with dedicated mining technology
mining pool	A consortium of miners
mining	The activity of recording blocks of transactions on the blockchain
mem-pool	Set of pending transactions received by a miner
proof-of-work (PoW)	A blockchain protocol based on computationally intensive record keeping
proof-of-stake (PoS)	A blockchain protocol based on a funds staking mechanism
satoshi	A Bitcoin token containing 10^{-8} bitcoins
stale block	A block lying in an abandoned chain
SHA-256	A common encryption algorithm

Appendix E Figures

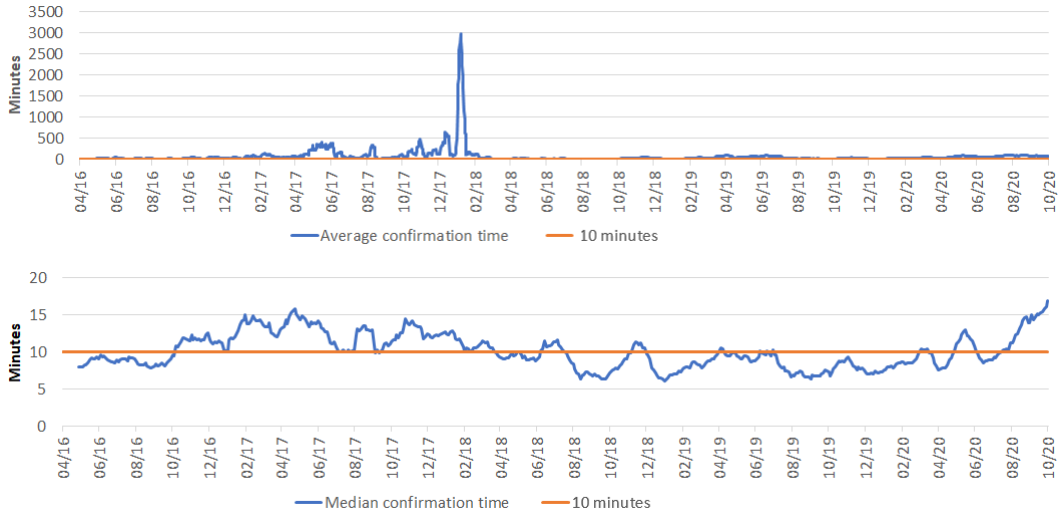

Figure 1: Average and median Bitcoin confirmation time ♦

Day-level data origin: https://www.blockchain.com/
Data smoothing preformed via moving average with 10 lags.

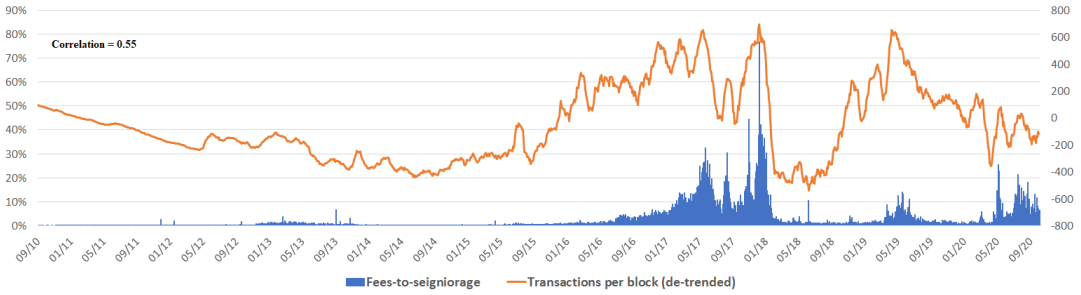

Figure 2: Fees-to-seigniorage ratio (in USD) and block transaction count for Bitcoin ♦

Day-level data origin: https://www.blockchain.com/
Value "0" of the de-trended series corresponds to approximately 800 transactions.
Data smoothing performed via moving average using 3 lags for "Fees-to-seigniorage" and 10 lags for "Transactions per block (avg)"

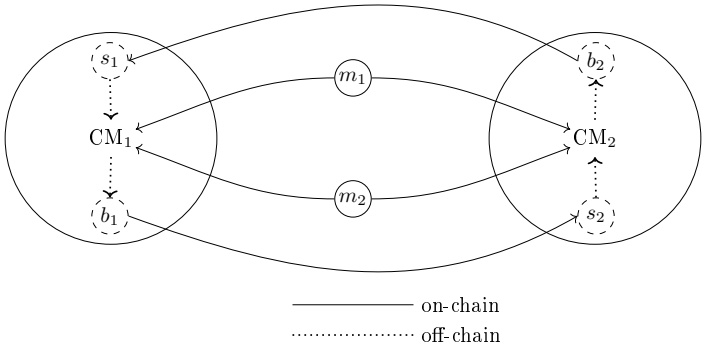

Figure 3: On-chain and off-chain transactions ♦

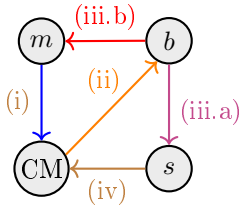

Figure 4: Circulation of a token ♦

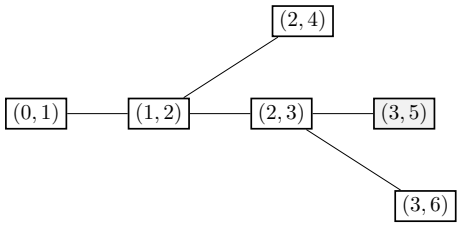

Figure 5: Longest Chain Rule (LCR) ♦

A branched block tree. Blocks are identified with height (left-index) and the rank of their publication time (right-index). Among the three chains that form the block tree, LCR selects the longest chain terminating with block $(3,5)$. Notice that the chain ending with block $(3,6)$ is one of the longest but was published later than the consensus chain, whereas the chain ending with block $(2,4)$ was published previously than the consensus chain but is shorter.

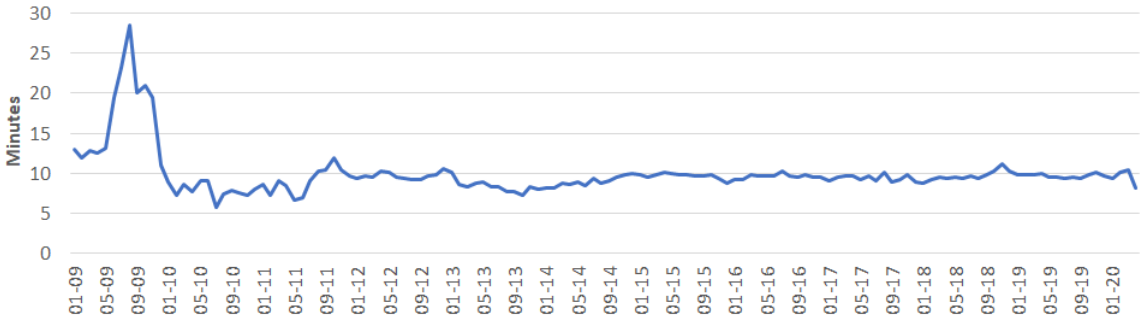

Figure 6: Block mining time (average) ♦

Month-level data from https://data.bitcoinity.org/bitcoin/block_time/all?f=m10&t=l

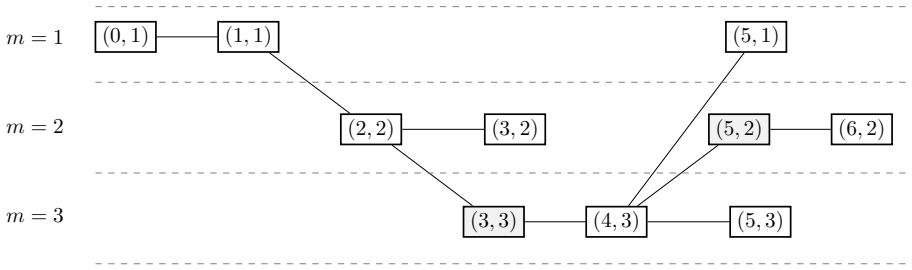

Figure 7: Three miners updating a blockchain ♦

Blocks are indexed $(h - h_0, m)$ for $m \in \{1, 2, 3\}$ and $h - h_0 \in \{0, 1, 2, 3, 4, 5, 6\}$, with $h_0 > 0$. Forks occur at $h - h_0 \in \{3, 5\}$ and are resolved according to LCR that selects as reference block among the head blocks of competing (longest) chains the one with the shortest update time (in gray).

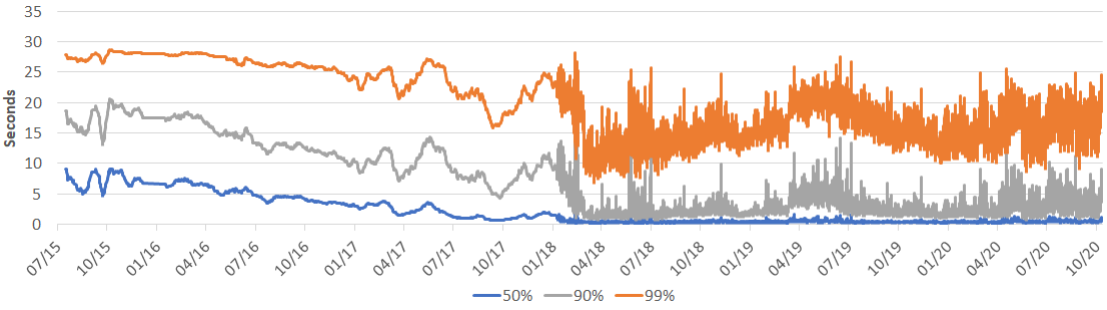

Figure 8: Block propagation time (% of total miners reached)* ♦

*Average time until a block is announced by a given percentage of total Bitcoin miners.

Day-level data origin: https://dsn.tm.kit.edu/bitcoin/#propagation
Data smoothing preformed via moving average with 15 lags.
All observations are averages of block propagation times recorded within a time span of approximaly one hour recorded between 12AM and 2PM.