Review of Economic Studies (2021) **0**, 1–30 doi:10.1093/restud/rdab014

Advance access publication 13 March 2021

Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System

GUR HUBERMAN
Columbia Business School
JACOB D. LESHNO
University of Chicago Booth School of Business
and
CIAMAC MOALLEMI
Columbia Business School

First version received March 2019*; Editorial decision December* 2020*; Accepted March* 2021 (*Eds.*)

Bitcoin provides its users with transaction-processing services which are similar to those of traditional payment systems. This article models the novel economic structure implied by Bitcoin's innovative decentralized design, which allows the payment system to be reliably operated by unrelated parties called miners. We find that this decentralized design protects users from monopoly pricing. Competition among service providers within the platform and free entry imply no entity can profitably affect the level of fees paid by users. Instead, a market for transaction-processing determines the fees users pay to gain priority and avoid transaction-processing delays. The article (i) derives closed-form formulas of the fees and waiting times and studies their properties, (ii) compares pricing under the Bitcoin Payment System to that under a traditional payment system operated by a profit-maximizing firm, and (iii) suggests protocol design modifications to enhance the platform's efficiency. The Appendix describes and explains the main attributes of Bitcoin and the underlying blockchain technology.

Key words: Antitrust, Open Source, Market design, Queueing, Payment Systems, Cryptocurrency, Distributed Ledger.

JEL Codes: D47, L17, E42, L4.

1. INTRODUCTION

The 2018 revenue of the global payment industry was $1.9 trillion (McKinsey and Company, 2019). The recipients of this revenue—payment-processing firms—enjoy network effects and economies of scale, and therefore limited competition and barriers to entry (Rosenbaum *et al.*, 2017; Morningstar, 2019). Multiple lawsuits against payment-processing firms accuse them

The editor in charge of this paper was Adam Szeidl.

of abusing their market power and harming welfare.[1] Moreover, regulators worldwide impose restrictions on payment-processing firms, in particular, capping the fees charged to users.[2]

The Bitcoin Payment System (BPS), a platform that provides payment services, shows the feasibility of an alternative, decentralized design. It has been operating reliably since its early 2009 inception. It is not controlled by any entity, governed by a computer protocol and obtains the required computer infrastructure from anonymous, independent profit-maximizing parties called "miners." Anyone with the required computational power and an internet connection can become a miner and compete with other miners to provide transaction-processing services to the platform and collect the associated rewards.

We model this novel economic structure and show that the BPS's decentralized design offers a prototype of a payment system in which users are protected from monopoly harm even if the payment system were a monopoly.[3] Free entry and competition of service providers *within platform* renders the service providers (*i.e.* the miners) unable to profitably affect the fees users pay. Even a miner who controls a large fraction of the computational power cannot profitably affect fees. Moreover, the fees users pay do not increase if users lose their alternative payment methods. Standard economic arguments suggest that weak competition among monopolistic firms calls for regulation to mitigate monopoly harm. Under the BPS, users are protected from abuses of monopoly power even without competition from other payment systems. Thus, the BPS addresses potential antitrust concerns in a novel, even revolutionary, way.

In the absence of a price-setting firm, the BPS relies on a market mechanism encoded in its protocol to determine prices and infrastructure. Our analysis of the protocol reveals inefficiencies in this market mechanism. Among them is the lack of a mechanism that drives the level of resources acquired and deployed to an efficient level, however defined. We provide design suggestions to address these concerns.

The model elaborates on the observation that the blockchain design makes the BPS a two-sided platform whose constituencies are: (i) miners who collectively provide the system's infrastructure in return for payment; (ii) users who transfer funds to others and pay fees. A brief description of the system is in order to explain the particular properties of this two-sided market that are the focus of our model. For concreteness, we focus on the BPS, whose basic design features are shared among most other cryptocurrencies. Appendix A provides a more detailed description of the BPS which is targeted for economists.

Users post transactions over time; miners organize them into blocks, each block with the same, limited capacity; the block of a single randomly selected miner is added to the blockchain; this block selection amounts to processing of the transactions in that block; the timing of miner selection is a Poisson process with a fixed rate which is independent of the aggregate computing

1. For example, see concerns discussed by Herkenhoff and Raveendranathan (2020), and Table 5 therein which provides a list of antitrust lawsuits against credit card payment networks and banks. In a congressional testimony, Aaron Klein (2020) argues that payment systems adopt fee structures that disadvantage the poor. See Evans and Schmalensee (2005) for a detailed description of the payment cards industry.

2. Hayashi and Maniff (2019) provide a long list of regulatory actions limiting credit card fees in countries around the world. Wright (2012) provides support for the concerns of a long list of public authorities and economists that the fee structure in debit and credit cards leads to inefficiency. In fact, according to Visa Inc. Fiscal 2019 Annual Report, "An increasing number of jurisdictions around the world regulate or influence debit and credit interchange reimbursement rates in their regions. For example, the Dodd–Frank Wall Street Reform and Consumer Act (Dodd–Frank Act) in the U.S. limits interchange reimbursement rates for certain debit card transactions, the European Union's (EU) IFR limits interchange rates in Europe (as discussed below) and the Reserve Bank of Australia and the Central Bank of Brazil regulate average permissible levels of interchange."

3. The attribution of monopoly power to the BPS is a thought experiment, not an empirical claim.

resources used by the miners.[4] That, and the fixed capacity of the blocks imply that the BPS has a fixed expected transaction-processing capacity.

The system's limited capacity coupled with the randomness of transaction arrival and processing times imply that, at times, transactions will be processed with delays of random lengths. To make the presentation cleaner, we assume, that on average, the system has sufficient capacity to process all transactions. In addition, the analysis assumes that the mining resources are sufficient to guarantee the system's reliability and security. When so, increases in the mining resources do not affect the system's transaction-processing capacity.

All miners perform the same tasks. Participation in the miner selection tournament is the most resource-consuming among these. A miner's chance of being selected is proportional to his share of the total computational resources. The selected miner is said to have mined a block, and is rewarded with a fixed, system-generated reward plus the fees associated with the transactions in that block. Each user chooses the fee associated with his transaction. Each miner is free to enter and exit the system at no cost. Each participating miner chooses which transactions to include in his block.

We set up a model of fees, priority levels, and mining intensity that captures the main features of the BPS. Its analysis highlights differences between the BPS and a traditional payment system operated by a profit-maximizing firm. The analysis delivers explicit formulas of the fees and delays, thereby enabling suggestions for design improvements. Figure 1 suggests an agreement between the fee formula and the data.

Beyond the quantitative results, the analysis offers a series of qualitative insights as follows.

The BPS processes all transactions, albeit with delay; all users receive strict positive surplus. In contrast, in our setting a profit-maximizing firm excludes low willingness to pay (WTP) transactions but processes the rest without delay. In the BPS, the fee level does not increase if user WTP increases (*e.g.* if users lose their alternative options) whereas the firm charges more if users' WTP increases.

User payments under the BPS are determined by a congestion market and are payments for service speed. A profit-seeking miner excludes the transactions which offer the lowest fees when the assembled block is full. Therefore, users to whom delays are costly will offer relatively high fees to gain priority and be served faster.

In equilibrium, users with higher delay costs receive higher processing priority and therefore shorter delays. The fee a user pays is equal to the expected delay externality he imposes on others who offer lower fees. Thus, fees are equal to those obtained by allocating priority through a Vickrey–Clarke–Groves (VCG) mechanism, although the BPS employs no auctioneer. User WTP does not affect fees, assuming WTP is sufficiently high. This implies users are protected from price increase should alternative payment service providers leave the market.

An increase (respectively, decrease) in the arrival rate of new transactions results in increased (respectively decreased) congestion, which in turn causes fees to be higher (respectively lower). No delays imply no fees. The analysis offers an explicit relation between block size (which reflects congestion) and the USD-denominated fee. Figure 1 provides a theoretical and an empirical summary of this relation. Notably, the dependence of fees on congestion is highly non-linear: fees are negligible when blocks are below 50% of their maximal size, positive when blocks are at 80% of their maximal size, and substantially higher when blocks are close to their maximal size.

We show that even a miner who controls a substantial fraction of the mining resources cannot profitably affect the fees paid by users. While a large miner can affect a user's choice of fees, an increase in user fees will attract entry by new miners, leading to increased competition and lower

4. This is a simplification, see Appendix A for a precise description.

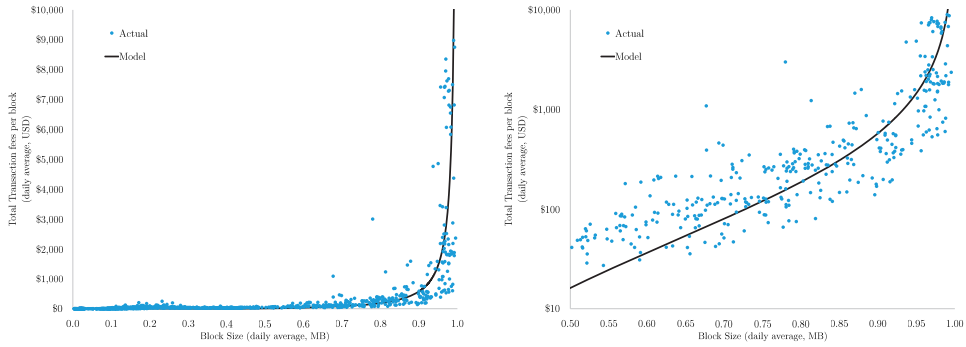

FIGURE 1

Actual and model predicted transaction fees per block (in USD) and block size for the Bitcoin Payment System (daily averages, 1 April 2011 – 30 June 2017). The chart on the left shows fees on a linear scale from the entire range of dates; the chart on the right shows fees on a logarithmic scale over periods when block size was above 0.5 MB. See Section 6.2 for details.

profits for a miner who attempts to affect user fees. In contrast to standard platform competition, new miners face no barriers to entry as they enter and compete within the same platform. Free entry of miners is essential to this result.

Newly minted coins and transaction fees fund the miners who acquire mining resources in USD-denominated markets. Exchange rate and fee-level fluctuations affect miners' aggregate income, which in turn affects aggregate mining power in the BPS. There is no mechanism that drives the level of infrastructure resources acquired and deployed to an efficient level, however defined.

The analysis points to an efficiency contrast between the BPS and a profit-maximizing firm. Namely, the latter's service is associated with dead-weight loss, whereas the BPS can operate with excess capacity, serving all users and awarding each with strictly positive surplus. If miners are homogeneous, all surplus accrues to the users.

However, the costs of operating the BPS are likely to be higher than those of a traditional firm: its decentralized architecture requires duplication of computations and expenditure of efforts in the miner selection tournament; the aggregate mining level can be too high; costly delays are necessary to induce users to pay transaction fees. Thus, welfare under the BPS can be higher or lower than that under a traditional system, depending on the value of eliminating monopoly dead-weight loss.

Hundreds of variants of Bitcoin have emerged, with many aiming to improve on the original Nakamoto (2008) design. Our analysis provides the following messages to designers. First, it suggests that congestion is not merely an engineering necessity but also a device to motivate users to pay transaction fees. Second, the analysis suggests a simple modification that avoids the variation in revenue from transaction fees. In the BPS, capacity is fixed and congestion varies with demand; consequently, the revenue and infrastructure levels vary over time.

We suggest an improved design: a protocol rule that automatically adjusts the system's capacity according to the volume of transactions, thereby steadying congestion, aggregate fees, and mining level. This design has two advantages over alternatives such as a fixed transaction fee: (1) it allows the system to raise revenue without excluding transactions, as users can choose to pay no fees but incur delays; (2) it allows the protocol to obtain the USD market value of delay reduction without the need to learn the exchange rate. Alternatives such as fixed transaction fees (or newly minted

coins) need to be set within the protocol and be denominated in the system's coin, implying revenue fluctuation with the coin's exchange rate.

The analysis also allows us to optimize parameter choices. We offer an analytic expression for the delay costs required to raise a certain revenue level. Analysis and examples suggest that large blocks are less efficient in that they require longer delays to sustain a given level of revenue.

1.1. *Related literature*

Famously, a white paper by Nakamoto (2008) coined the term Bitcoin and described the BPS. Its opening paragraph criticizes the costs of the existing financial system and its usefulness to small transactions, "Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions." Section 6 ("Incentive") predicts that transaction fees will eventually fund the system, "The incentive can also be funded with transaction fees… Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees…" The section's title notwithstanding, Nakamoto (2008) is silent on the incentive to pay transaction fees, their relation to other parameters, and their implications; understanding these is the present article's task.

Kroll *et al.* (2013) offer an analysis of the incentives faced by participants in the system, and especially the incentives faced by miners. They conclude a brief discussion of transaction fees by stating, "We therefore do not expect transaction fees to play a significant long-term role in the economics of the Bitcoin system, under the current rules. We believe that a rules change would be necessary before transactions fees can play any major role in the Bitcoin economy." The present article shows otherwise, *i.e.*, that transaction fees have dual and crucial roles in the Bitcoin system: (1) they are supplanting newly minted coins as the funding source of the mining community; (2) they are the arbiters of priority in the congestion of messages to be processed by the miners, *i.e.*, they determine priority in the message queue.

Following the initial version of this article, the design of transaction fee mechanisms has received attention from both academics and practitioners (*e.g.* Buterin, 2018). Easley *et al.* (2017) is a contemporaneous piece which proposes and empirically examines an equilibrium model of exogenously specified transactions fees and block size assumed restricted to a single transaction. Their model predicts that miners' profits are zero and that fees are positively correlated with transaction waiting times. The data appear consistent with these predictions. Lavi *et al.* (2017), Yao (2018), and Basu *et al.* (2019) suggest alternative mechanisms for transaction fees.

Prat and Walter (2018) study the dynamics of miner entry as it is influenced by changes in exchange rates and technological changes and predictions thereof. Felten (2013) argues that in equilibrium miners break even. Cong *et al.* (2018) argue that large mining pools confer risk-sharing advantages on their members, which are mitigated by the larger fees which larger pools charge their members. Arnosti and Weinberg (2018) develop a model where miners are heterogeneous in their cost structure, and quantifies how such asymmetries lead to the formation of oligopolies and concentration of mining power.

Eyal and Sirer (2014) and Sapirshtein *et al.* (2016) analyse the equilibrium between miners and show that proper design of the blockchain protocol produces a reliable system in equilibrium if all miners are sufficiently small. Babaioff *et al.* (2012) analyse the incentives to propagate information in the BPS. Leshno and Strack (2020) and Chen *et al.* (2019) provide axioms to capture free entry of miners and their implication for miner selection. Narayanan *et al.* (2016) offer an elaborate description and analysis of the system. Croman *et al.* (2016) provide cost estimates for the BPS and analyse the potential for transaction-processing capacity. Eyal *et al.* (2016)

suggest an alternative design aimed to construct a system with a higher capacity. Carlsten *et al.* (2016) analyse how incentives for miners change when miners are rewarded with transaction fees instead of newly created coins. Chiu and Koeppl (2017) evaluate the welfare implications of printing new coins.

The protocol proposed by Nakamoto (2008) posits that in case of a fork, miners will follow the longest branch. Biais *et al.* (2018) study the robustness of this rule. Budish (2018) studies the system's vulnerability to attacks and argues that the cost of securing Bitcoin is inefficiently high. Abadi and Brunnermeier (2018) posit three desired properties of distributed ledger technologies, (1) correctness, (2) decentralization, and (3) cost efficiency and argue that no ledger can satisfy all three properties simultaneously.

Yermack (2015) reviews the history of Bitcoin and its price history to "argue that bitcoin does not behave much like a currency according to the criteria widely used by economists. Instead bitcoin resembles a speculative investment similar to the Internet stocks of the late 1990s."

Gandal and Halaburda (2014) analyse competition between the different cryptocurrencies. Halaburda and Sarvary (2016) review the cryptocurrency market, its development, and future potential of blockchain technology. Gans and Halaburda (2015) analyse the economics of digital currencies, focusing on platform-sponsored credits. Catalini and Gans (2020) discuss possible opportunities that can arise from blockchain technology. Huberman *et al.* (2019) provide a broader comparison between services provided by the BPS and services provided by a firm.

Recent work considers the valuation of bitcoin relative to fiat currencies and other goods. That work usually assumes away the limited capacity of the BPS, although it induces delays and transaction fees. Ron and Shamir (2013) and Athey *et al.* (2016) provide analysis of the usage of bitcoin and its value as a currency. Schilling and Uhlig (2018) analyse the evolution of bitcoin prices relative to fiat currency and its implications for monetary policy. Makarov and Schoar (2018) report arbitrage opportunities across cryptocurrency exchanges, primarily across regions.

Cong *et al.* (2018) study a dynamic pricing and adoption model in which wider adoption renders the cryptocurrency more valuable. Pagnotta and Buraschi (2018) study bitcoin pricing under the assumption that, at all levels, higher aggregate mining effort delivers higher value to users. Sockin and Xiong (2018) propose a pricing model for an ICO for a platform on which households can exchange certain goods or services if they own the platform's native coin.

Lui (1985), Glazer and Hassin (1986), Kittsteiner and Moldovanu (2005), and Hassin (1995) study a queuing system in which users with different waiting costs volunteer to pay transaction fees (termed bribes in Lui (1985) to gain priority in a queue to a single service station which serves customers one at a time. The main observation of Lui is that the server may increase its profits by increasing the speed of service. Hassin (1995) shows that the service rate that maximizes the server's profits is always slower than the socially optimal service rate. Hassin and Haviv (2003) provide a summary of the results, and Hassin (2016) provides an updated review. Kittsteiner and Moldovanu (2005) show that convexity or concavity of delay costs determines the queue-discipline.

The present analysis considers a queuing system in which transaction arrival and service arrival is stochastic, but the service is processed in batches of fixed maximal size. The prior work corresponds to a batch size of one. The interaction among arrival rates, service rates, and the maximal batch size, and their impact on the transaction fees and server's revenues are of major concern.

1.2. *Organization of the article*

Section 2 provides a model of traditional payment systems, the BPS, and users who may use either. For the sake of completeness, Section 3 provides the standard analysis of a traditional

payment systems operated by a firm. Section 4 provides our main analysis and characterizes the equilibrium under the BPS. Section 5 leverages our analysis to provide design suggestions. Section 6 brings empirical evidence to bear on some of the model's predictions. Section 7 provides some final remarks. Appendix A provides a simplified explanation of the BPS and the underlying blockchain technology.

The Supplementary Appendix contains all omitted proofs and additional discussion. Supplementary Appendix B extends our analysis of the BPS to parameters where the participation constraint of some users binds. Supplementary Appendix C extends our analysis to allow for endogenous determination of the user's WTP. Supplementary Appendix D gives additional properties of transaction fees under the BPS. Additional figures are in Supplementary Appendix E. Omitted proofs are in Supplementary Appendix F.

2. ECONOMIC MODEL OF TRADITIONAL PAYMENT SYSTEMS AND THE BITCOIN PAYMENT SYSTEM

This section sets up a model of a payment system to facilitate a comparison between a decentralized protocol like Bitcoin and a conventional payment system which is controlled by a profit-maximizing firm. Section 2.1 describes the users. Their preferences are the same across the two payment systems. Section 2.2 briefly states the familiar problem of a firm providing payment services. Section 2.3 describes succinctly the features of the Bitcoin Payment System (BPS) relevant to its economic analysis and its comparison with a traditional system. Sections 3 and 4 offer equilibrium analyses of the firm and of the BPS, respectively.

2.1. *Users*

Each user has a single potential transaction; hence, references to users and their transactions are interchangeable. Users are heterogeneous in two distinct dimensions. First, users differ in their willingness to pay (WTP) for using the system. The value a user derives from sending a transaction in the system above the value available via an alternative is his WTP $R = v - v_{\text{alt}}$. Second, users have different delay costs per unit time c. The net reward of user (R, c) from sending a transaction that is processed after delay W and paying a transaction fee b is

$$u(W, b \mid R, c) = R - c \cdot W - b. \tag{1}$$

The variables R and b are denominated in USD;[5] the variable c is in USD per unit time. By the definition of R, a potential user will prefer using the system over the alternative (outside option) if $u(W, b \mid R, c) \geq 0$.

To make the cleanest distinction between the systems, we consider a setting where $R \in \{R_L, R_H\}$ $(R_L \leq R_H)$ and is not correlated with c.[6] One interpretation is that users with WTP R_H have no compelling alternative of making the transfer, and therefore their WTP R_H is almost the entire value of processing the transaction, while users with WTP R_L can use an alternative method, and therefore their WTP is equal to the cost of the alternative method.

5. In practice, transaction fees in the BPS are denominated in bitcoin. However, since users decide transaction fees as they submit transactions, we will consider them as USD denominated without loss of generality. This is in contrast to the block reward S discussed in Section 2.3, which is fixed by the protocol, and hence is impacted by the USD/bitcoin exchange rate.

6. An alternative and analogous model entails $u = V\delta^W - b - v_{\text{alt}}$. Variation in R is variation in v_{alt}. Variation in c is variation in δ. All have the same V.

WTP reflects various features of the system. Currently, users of the BPS face costs and risks due to the volatility of the bitcoin to USD exchange rate. Likewise, users may have concerns about the long-run viability of the system, security, privacy, or ease of use (*e.g.* the lack of password recovery service). On the other hand, the BPS may facilitate transactions that are difficult to conduct through other means. We capture such considerations by the WTP R.

Potential users arrive over time according to a Poisson process. The arrival rate of users with value R_j is λ_j with $j=L,H$ and $\lambda=\lambda_L+\lambda_H$. Both of these user populations have heterogeneous delay costs per unit time c that are distributed $c\sim F[0,\bar{c}]$, independently of the user's WTP R. The cumulative distribution function $F(\cdot)$ has a density $f(\cdot)$, and its tail probability is $\bar{F}(c)\triangleq 1-F(c)$.

For tractability, users know the steady-state behaviour of the system, but do not observe other pending transactions at the time they submit their transaction. Users are risk neutral and maximize their expected net reward.

We focus our analysis on the case summarized below which gives the cleanest distinction between the BPS and a firm.

Assumption 1. *The following hold:*

- $\lambda_H R_H > (\lambda_L+\lambda_H)R_L$
- $R_H \geq R_L > \bar{R} > 0$ *where* $\bar{R}$ *is defined in Lemma 2.*
- *User delay costs c are distributed independently of WTP R.*

The assumption that $R>0$ entails that transaction processing by the BPS is valuable to its potential users after accounting for exchange-rate risk, the BPS's other limitations, and the possibility of using alternative systems. In particular, users consider the system to be a reliable means of sending transactions.

2.2. *Payment system run by a firm*

A firm-run conventional payment system can process transactions without delay at a marginal cost of c_f per transaction. The firm sets its price in response to the distribution of consumer demand. The firm faces no capacity constraints, can costlessly delay transactions and can offer different prices for processing transactions with different delays. In Section 3, we show that the firm does not pursue these policies because they do not increase its profit.

2.3. *Decentralized cryptocurrency*

The BPS offers users a similar functionality to that offered by familiar payment systems, *i.e.*, the ability to transfer balances from one user to another. In contrast to traditional payment systems, the BPS uses a decentralized network of computers (so called miners) to process transactions and maintain the ledger containing their history. The novel blockchain design ensures the system as a whole is reliable and trustworthy without the need to trust any individual miners.

A computer protocol governs the system and dictates the rules for how miners and users interact within the system. Thus, the BPS system is a two-sided market with rules that are fixed by a computer protocol. The description in Appendix A provides further details regarding the protocol's operations and functionality. In this section we provide the implications of the design for the structure of the two-sided market.

Users send their transactions as they would under any payment system but also select the transaction fee they will pay. Transactions need not be processed in their order of arrival. Processing may take time.

Miners provide their computational infrastructure to the BPS at will and can switch between being active and inactive. Collectively, the miners maintain a ledger of all transaction history. Transactions are periodically added to the ledger in batches, in the form of a block of transaction data. These additions are according to a Poisson process[7] with rate μ, irrespective of the number of miners. For each block, a randomly chosen active miner selects which pending transactions are processed in the block. That miner is said to have mined the block. The probability that a miner is chosen is equal to his share of the total computational power. A block can contain up to K transactions.[8] Pending transactions not included in a block wait to be processed in a future block. Miners observe all pending transactions and the fees associated with them. Each miner applies his own selection of up to K pending transactions. We say that transactions included in the miner's block are processed by that miner.

Miners incur a cost per unit time while they are active. A miner who mines a new block is rewarded with the transaction fees paid by the transactions included in that block as well as a fixed block reward of newly minted coins. We denote by S the expected number of coins the system awards per unit time.[9] We use e to denote the USD/bitcoin exchange rate, which we assume fixed and exogenous. Of particular interest will be the case where $S=0$, which describes the operation of the BPS in the long term.[10]

Each miner chooses the computation power it deploys. We denote the aggregate computational power by N. The total expected processing capacity of the system is an average μK transactions per unit time. The values μ, K are predetermined by the protocol and are unaffected by the number of miners, their total computational power N, or the transaction volume λ.

Realized processing capacity is random because block arrival time is random. The load parameter is $\rho=\lambda/\mu K$, which is the ratio of average demand to capacity. The parameter ρ is a measure of the system's congestion. To make the presentation cleaner, we assume, that on average, the system has sufficient capacity to process all transactions. Supplementary Appendix B covers the case $\rho>1$.

Assumption 2. *The system has sufficient capacity to eventually process all transactions, that is,* $\rho<1$.

Miners who possess a small fraction of the total computational power N have a small probability of mining a block. We assume that each of these miners cannot influence the system or the choices of other miners and users. We refer to these as small miners. To capture that each small miner has a negligible effect on transaction-processing delays, the model distinguishes between large miners and small miners. Each large miner i can choose to deploy computational power $x_i \geq 0$. When taking actions, each of these large miners takes into account the actions' impact on the system, including the way they influence other actors' choices. We assume there are finitely many large miners indexed by i, each with computational power bounded by $\bar{x}_i \in \mathbb{R} \cup \{\infty\}$ and a cost of computational power $c_i : [0, \bar{x}_i) \to \mathbb{R}$ that is smooth, increasing, strictly convex, and satisfies $c_i(0)=0$, $\lim_{x \to \bar{x}_i} c'(x) = \infty$. There are infinitely many small miners, and each small miner who chooses to be active deploys an identical, infinitesimal amount of computational power at infinitesimal cost $c_m > 0$. If selected to mine a block, the miner's revenue from the block does not depend on the computational power he deploys.

7. A Poisson process is the limit of many independent binomial trials. See footnote 30.
8. While in practice transactions may vary in size, for the sake of tractability, we assume all transactions are of the same size.
9. Note that all values are given per unit time.
10. In the BPS, the block reward is halved every 4 years, until it is rounded down to 0.

A miner's block assembly policy $A \in \mathcal{A}$ captures his transaction selection. Formally, the collection of pending transactions is associated with a list of transaction fees $\boldsymbol{b} = (b_1, \ldots, b_n)$. The block assembly function A assigns for every $\boldsymbol{b}$ a vector $A(\boldsymbol{b})$ of zeros and ones of the same length; transaction j is included in the block if the corresponding entry of $A(\boldsymbol{b})$ is one. Compliance with the protocol requires that the vector $A(\boldsymbol{b})$ has no more than K entries equal to one.

Next, we describe the interactions between users, between miners (large and small), and across these two groups. Users play a congestion queueing game, in which each user chooses b, the fee he offers, to maximize his expected utility (1). A user's delay W depends on the selection of transactions by a randomly chosen miner. That selection is sensitive to the fee offered by the transaction and its level relative to other transaction fees. Each miner is a profit maximizer who chooses whether to be active or not; those who choose to be active choose a block assembly policy. Large miners who choose to be active also choose their computational power. Miners may enter or exit in response to profit opportunities, leading to an increase or a decrease in the total computational power. An increase in the total computational power lowers the probability a given miner is chosen to mine a block, and therefore lowers the miner's payoff. Large miners' block assembly policies can affect the transaction fees offered by users.

Behaviours in systems like the one we are studying could be time- and state-dependent. We abstract from both. We focus on equilibria such that the system is time invariant and has a steady-state distribution. We assume all participants know the system parameters and steady-state distribution. We imagine the equilibria being on a time horizon where the model parameters (arrival rates, exchange rate, etc.) are fixed. Over a longer time horizon these parameters may be changing, and hence the system may move from one equilibrium to another.

Formally, we study the three-step, extensive-form game which summarizes the interactions among the various actors. These steps are:

(i) Each large miner i chooses whether to be inactive or to be active with some computational power $x_i > 0$ and some block assembly policy $A_i \in \mathcal{A}$.

(ii) Small miners observe the actions taken by the large miners in the first step and choose whether to be inactive, or to be active with infinitesimal computational power and some block assembly policy A. For each $A \in \mathcal{A}$, let $\eta(A)$ be the aggregate computational power of the miners (small and large) who choose a block assembly policy A, *i.e.*, η is the distribution of block assembly policies. The aggregate of $\eta(A)$ is N. The probability a block is assembled according to A is $\eta(A)/N$.

(iii) Users play the congestion queueing game implied by η. We restrict attention to deterministic stationary strategies. A user's expected waiting time depends on the fee he offers, the fraction γ of users who participate, and the distribution of transaction fees $G(\cdot)$. Each user type (R, c) chooses whether to opt out and receive a payoff of 0, or participate and send a transaction with fee $b(R, c) \geq 0$ to receive his expected steady-state payoff,

$$R - b(R,c) - c \cdot W(b(R,c) \mid G, \gamma, \eta),$$

where $W(b(R,c) \mid G, \gamma, \eta)$ is the expected waiting time for a transaction with fee $b(R,c)$ under the steady-state distribution of the system.[11]

11. The decisions of all participants specify a continuous time Markov process and its steady-state distribution as follows. The states are lists of transaction fees of pending transactions $\boldsymbol{b} = (b_1, \ldots, b_n) \in \cup_n \mathbb{R}^n \cup \{\phi\}$. There are two kinds of transitions. At Poisson rate $\gamma\lambda$ a user arrives and posts a transaction with transaction fee independently drawn from G, and the state is updated by appending the new transaction. At Poisson rate μ a block is mined, and the block assembly policy $A(\cdot)$ is applied with probability $\eta(A)/N$. The system transitions to a new state by erasing all transactions selected by $A(\cdot)$. For completeness, if given G, γ, η the system does not have a steady-state distribution, we set $W(\cdot \mid G, \gamma, \eta) \equiv \infty$.

The payoff of an active large miner i with computational power $x_i > 0$ and block assembly policy A_i is

$$\frac{x_i}{N}\Big(\mathrm{Rev}(A_i \mid G, \gamma, \eta) + e \cdot S\Big) - c_i(x_i),$$

where $c_i(x_i)$ is large miner i's cost of computational power, and $\mathrm{Rev}(A \mid G, \gamma, \eta) = \mathbb{E}_{\boldsymbol{b}}\left[\boldsymbol{b} \cdot A(\boldsymbol{b})\right]$ is the expected transaction fees per block assembled by A under the steady-state distribution of pending transactions $\boldsymbol{b}$.[12] The payoff of an active small miner with block assembly policy A is proportional to

$$\frac{1}{N}\Big(\mathrm{Rev}(A \mid G, \gamma, \eta) + e \cdot S\Big) - c_m,$$

where all small miners have the same cost of an infinitesimal unit of computational power $c_m > 0$. All inactive miners receive a payoff of 0.

Assumption 3. *Given any feasible profile of choices by large miners, in any subgame perfect equilibrium of the induced subgame for small miners and users there are some small miners that are active and some small miners that are inactive.*

Assumption 3 requires the presence of sufficiently many players who can become active small miners. This is likely to be satisfied if it is possible to become a small miner by buying standard computational resources on the open market.[13] Because a miner's payoff decreases with aggregate computational power, this implies that in any equilibrium some potential small miners are inactive. The second part of Assumption 3 requires that some small miners are active given any choices by large miners. This will be satisfied if the total computational resources employed by large miners are limited, and the computational resources used by small miners are sufficiently efficient (*i.e.* c_m sufficiently small).

To highlight the distinctive properties of the system, the analysis focuses on the parameter range where all potential transactions can be processed. The assumptions in Section 2.1 imply that there are sufficiently many miners for the system to operate reliably and securely. In Section 4, we analyse the BPS under these assumptions and verify when they indeed hold.

To avoid technical issues with equilibrium existence, we restrict the set of block assembly policies $\mathcal{A}$. We require that for any profile of large miners' block assembly policies chosen from $\mathcal{A}$, the induced subgame (played by small miners and users) has at least one subgame perfect Nash equilibrium in pure strategies. We restrict attention to deterministic strategies and implicitly assume that small miners can use a public coordination device to coordinate their entry decisions.

Miners procure the resources they need in fiat currency-denominated markets. Therefore, we consider all payments and costs denominated in USD rather than in bitcoin. In particular, the USD value of the block reward fluctuates with the exchange rate. No miner can affect this exchange rate.

3. ANALYSIS OF THE FIRM

The firm's problem is standard and stated here for completeness. We consider the profit-maximizing mechanism, allowing for probabilistic or dynamic mechanisms. By the revelation

12. The distribution of pending transactions observed by a miner who is selected to mine a block is identical to the steady-state distribution of pending transactions. For completeness, if given G, γ, η the system does not have a steady-state distribution we set $\mathrm{Rev}(A \mid G, \gamma, \eta) \equiv 0$.

13. A miner who controls a sufficiently large fraction of the mining resources may behave in a way that disadvantages small miners (*e.g.* selfish mining; Eyal and Sirer, 2014). Our results hold as long as the miner is unable to prevent small miner entry.

principle, it is sufficient to consider direct mechanisms in which the firm offers a menu to each user. Since the firm faces no capacity constraints, it can optimize its menu separately for each user. Therefore, a menu of options that maximizes profit from a single randomly drawn user delivers the firm's optimal profit.

The following proposition shows that, unable to distinguish high and low WTP customers, the firm sets a transaction fee that precludes low WTP customers from using the system and processes all the transactions that pay this fee with no delay. The firm can and does change the price it charges if R_H changes.

Proposition 1. *When $\lambda_H R_H > (\lambda_H + \lambda_L) R_L$, the firm's optimal menu includes a single option: it charges the fee $b = R_H$ and processes all transactions that are willing to pay the fee with no delay. Thus, only high value customers are served. Consumer surplus is 0 and social surplus is $\lambda_H (R_H - c_f)$, all accruing to the firm.*

The intuition for the result is that the firm cannot use delays to screen between high and low WTP customers and therefore avoids delays that decrease a user's willingness to pay.[14] When $\lambda_H R_H > (\lambda_H + \lambda_L) R_L$, the firm makes higher profits by selling only to high WTP users. The proof is in Supplementary Appendix F.5.

A few observations facilitate the comparison with the BPS (presented in Section 4.3). First, the distribution of the user delay costs F is irrelevant to the equilibrium outcome when the firm is the service provider. Second, pricing out the low WTP customers entails a dead-weight loss of $\lambda_L (R_L - c_f)$. Third, the high WTP customers pay exactly their WTP. They will pay more, *e.g.*, if these customers lose their best outside option.

The firm's profit is likely to draw the attention of potential entrants seeking to establish a competing payment service. Such competing payment services provide agents with alternative options, thereby reducing their WTP R (the value of using the BPS relative to the alternative options) and the price the firm can charge. However, the strong network effects and high setup costs that characterize the payments industry are likely to deter entry.[15] Even if there are multiple payment providers in the market, as long as each serves a separate segment, the service providers enjoy pricing power.[16]

4. ANALYSIS OF THE BITCOIN PAYMENT SYSTEM

We analyse the equilibrium of the system under the assumptions stated earlier. Section 4.1 analyses the behaviour of miners in steps (i) and (ii). Section 4.2 analyses the behaviour of users in step (iii). Section 4.3 completes the analysis, giving expressions for the system's infrastructure level and welfare.

4.1. *Miners, small and large*

A small miner's choice of block assembly policy does not affect the distribution of block assembly policies η and cannot affect users' fee choices. It follows that small miners maximize their payoffs

14. Recall that in our setting were there is no correlation between WTP and delay costs. Proposition 1 may not hold if such correlation exists.

15. See, for example, Morningstar (2019), Evans and Schmalensee (2005), and references therein.

16. Edelman and Wright (2015) argue that price coherence of payment cards (*i.e.* the restriction not to surcharge for payment by card) results in inefficiency that is not mitigated by competition. Another illustration of the ability to exercise market power is Apple's ability to collect 15 basis points from each transaction using the iPhone's NFC capabilities (https://www.cardfellow.com/blog/introduction-to-apple-pay/, retrieved January 2020). See also https://qz.com/1726203/apple-is-suffocating-mobile-payment-rivals/.

by selecting the block assembly policy A^* that maximizes $A^*(\boldsymbol{b})\cdot\boldsymbol{b}$ for any $\boldsymbol{b}$. In words, $A^*(\cdot)$ selects the K pending transactions offering the highest fees. (If there are fewer than K pending transactions, $A^*(\cdot)$ selects all of them.)

A large miner's choice of block assembly policy affects the distribution of block assembly policies η, changing the induced subgame for small miners and users. It may seem as though large miners can attempt to increase their payoffs by choosing a block assembly policy different from A^* to favourably affect users' fee choices. However, Theorem 1 shows that such attempts will not increase the miners payoffs; entry by small miners renders the block assembly policy A^* optimal for any large miner.

Theorem 1 considers the choices of large miners' behaviour in step (i), fixing possible responses of small miners and users. That is, for any profile of choices of large miners, we select an equilibrium play of small miners and users in the resulting subgame. Each selection generates an induced game between large miners. We use x_i^* to denote the unique solution to $c_i'(x_i^*)=c_m$ or $x_i^*=0$ if no solution exists.

Theorem 1. *In any induced game between large miners, it is a dominant strategy for each large miner i to choose the block assembly policy A^* and the computational power x_i^*. Moreover, for any choice of computational power x_i, we have that A^*, x_i dominates A, x_i for any block assembly policy A.*

In the equilibrium in which all miners choose A^*, the total amount of computational power in the network is

$$N=\frac{\text{Rev}+e\cdot S}{c_m}, \tag{2}$$

where Rev *is the total transaction fees in USD paid by users per unit time and e is the USD/bitcoin exchange rate.*

Theorem 1 holds regardless of the number of large miners. In particular, free entry of small miners precludes large miners from profitably affecting transaction fees even if all large miners collude.

The proof relies on free riding by small miners. For example, large miner i may choose to process only transactions with a fee above b', leading to a subgame in which some users increase their transaction fees above b' to avoid being delayed when miner i is selected. If the increased fees outweigh the loss from not processing transactions with a fee lower than b', choosing such a block assembly policy can increase miner i's expected transaction fees per block. However, this creates a larger increase in the expected transaction fees per block of small miners because small miners benefit from the increased fees while still processing all transactions. Entry by small miners increases the aggregate computational power so that small miners break even. Because small miners collect more fees than a large miner attempting to affect fees, free entry implies the large miner either breaks even or is strictly worse off.

Proof. Consider an arbitrary profile of choices by large miners and a subgame perfect equilibrium of the induced subgame for small miners and users. By Assumption 3, there are small miners that are active. Consider such an active small miner. Since small miners are non-atomic, the small miner's choice of block assembly policy $A(\cdot)$ does not affect η or N. Therefore, it does not affect G,γ and the steady-state distribution of $\boldsymbol{b}$. Since for any fixed distribution of $\boldsymbol{b}$, we have that $\text{Rev}(A^*\mid G,\gamma,\eta)=\max_A\{\text{Rev}(A\mid G,\gamma,\eta)\}$, it is a best response for the active small miner to choose A^*. Furthermore, any block assembly policy that constitutes a best response must give the small miner the same payoff as A^*.

Also by Assumption 3, there are inactive small miners, and therefore small miners must be indifferent between being inactive or active with A^*,

$$\frac{1}{N}\left(\mathrm{Rev}\left(A^* \mid G,\gamma,\eta\right)+e\cdot S\right)-c_m=0,$$

yielding

$$\mathrm{Rev}\left(A^* \mid G,\gamma,\eta\right)+e\cdot S=c_m N. \tag{3}$$

Now consider a large miner i who can affect the distribution η and thereby affect G,γ. Let x_i, A_i denote the computational power and block assembly policy of miner i, respectively. Fix the choices of other large miners, fix $x_i \geq 0$, and let G^{A_i}, γ^{A_i}, η^{A_i}, and N^{A_i} be distributions and values induced by a subgame perfect equilibrium of the subgame induced by miner i's choice of A_i, holding all other choices by large miners fixed. We have that

$$\begin{aligned}
&\frac{x_i}{N^{A_i}}\left(\mathrm{Rev}\left(A_i \mid G^{A_i},\gamma^{A_i},\eta^{A_i}\right)+e\cdot S\right)-c_i(x_i)\\
\leq&\frac{x_i}{N^{A_i}}\left(\mathrm{Rev}\left(A^* \mid G^{A_i},\gamma^{A_i},\eta^{A_i}\right)+e\cdot S\right)-c_i(x_i)\\
=&\frac{x_i}{N^{A_i}}c_m N^{A_i}-c_i(x_i)\\
=&c_m x_i-c_i(x_i).
\end{aligned} \tag{4}$$

The inequality follows because holding G,γ,η,N fixed, A^* delivers higher revenue than any A. The first equality follows from (3).

For $A_i = A^*$, using (3), we have that

$$\begin{aligned}
&\frac{x_i}{N^{A_i}}\left(\mathrm{Rev}\left(A_i \mid G^{A_i},\gamma^{A_i},\eta^{A_i}\right)+e\cdot S\right)-c_i(x_i)\\
=&\frac{x_i}{N^{A^*}}c_m N^{A^*}-c_i(x_i)\\
=&c_m x_i-c_i(x_i).
\end{aligned}$$

We thus showed that given any profile of choices of other large miners and any best responses of users and small miners, miner i attains the maximal payoff of

$$\sup_{x_i}\{c_m x_i-c_i(x_i)\}=c_m x_i^*-c_i\left(x_i^*\right)$$

by selecting the block assembly policy A^* and the computational power x_i^* that is either the unique solution to $c_i'\left(x_i^*\right)=c_m$ or $x_i^*=0$ if no solution exists.

Consider a profile where all active small miners choose A^* and each large miner i chooses A^* and x_i^*. Denote by η^* the implied distribution of computational power, which is given by $\eta^*\left(A^*\right)=N$ and $\eta^*(A)=0$ for all $A\neq A^*$. Complete the description of the strategy profile by having small miners and users play some subgame perfect equilibrium following any possible deviation by a large miners. The arguments above show this profile constitutes a subgame perfect equilibrium, as large miners, small miners, and users all play a best response.

Since $\rho < 1$, all transactions are eventually processed and $\text{Rev} = \text{Rev}\left(A^* \mid G, \gamma, \eta^*\right)$ is equal to the total transaction fees (in USD) per unit time under a subgame perfect equilibrium of the induced subgame for users (which will be characterized in the next section). Rewriting (3), we have that

$$N = \frac{\text{Rev} + e \cdot S}{c_m}.$$

□

Large miners can make positive profits if their average cost per computational unit is below c_m.[17] For the case where large miners do not have a computational cost advantage, we obtain the following immediate corollary of Theorem 1.

Corollary 1. If all large miners have the same cost c_m per computational unit, that is, $c_i(x) = c_m x$ for all large miners i, then all miners make zero profit.

While choosing block assembly policy A^* is a weakly dominant strategy, we have not yet ruled out other equilibria in which large miners may choose other block assembly policies. To formally preclude other equilibria, we introduce a perturbation that ensures the distribution of pending transaction has full support. Let G_0 be a distribution with strictly positive density over $\mathbb{R}_+$ (*e.g.* the half-normal distribution). The ε-perturbed system is given by adding to the original game exogenous arrivals of transactions and blocks. Additional transactions arrive according to a Poisson process with rate ε, each with a fee independently drawn from G_0. Additional blocks arrive according to a Poisson process with rate ε, and these blocks process all pending transactions (regardless of their number). The ε-perturbed game is identical to the original game, except for payoffs being determined by the steady-state distribution of the ε-perturbed system.

We say that two block assembly policies A, A' are G_0-equivalent if $A(\boldsymbol{b}) = A'(\boldsymbol{b})$ with probability 1 for $\boldsymbol{b}$ that is generated by independently drawing a geometrically distributed number of transactions from G_0. Notice that if A, A' are G_0-equivalent, they are also payoff equivalent. For any $\varepsilon > 0$, the argument in the proof of Theorem 1 implies that any block mining policy A that is not G_0-equivalent to A^* is strictly dominated. Thus, the equilibrium described in Theorem 1 is the unique equilibrium (up to payoff irrelevant variations) that survives the perturbation.

Proposition 2. *For any $\varepsilon > 0$, in any subgame perfect equilibrium of the ε-perturbed game, all active miners choose the block assembly policy that is G_0-equivalent to A^*.*

Proof. Let $\text{Rev}(A \mid G, \gamma, \eta, G_0, \varepsilon)$ denote the expected transaction fees per block in the ε-perturbed game. If $A(\boldsymbol{b}) \neq A^*(\boldsymbol{b})$ with positive probability (given the steady-state distribution of pending transaction $\boldsymbol{b}$), we have that

$$\text{Rev}(A \mid G, \gamma, \eta, G_0, \varepsilon) < \text{Rev}\left(A^* \mid G, \gamma, \eta, G_0, \varepsilon\right).$$

Thus, we can replace the weak inequality in (4) with a strict inequality. Following the remainder of the proof of Theorem 1, it follows that x_i, A is strictly dominated by x_i^*, A^*. Finally, we have that if $A(\boldsymbol{b}) = A^*(\boldsymbol{b})$ with probability 1 (given the steady-state distribution of pending transaction $\boldsymbol{b}$) it must be that A, A^* are G_0-equivalent, since for any k there is a positive probability that a clearing block will be immediately followed by k arrivals of transactions drawn from G_0. □

17. For example, miners who position their servers near dams can have lower cost due to cheap electricity. If such opportunities are scarce and can support only a limited number of servers, they will not be competed away.

Entry by small miners is essential for Theorem 1. Suppose a single large miner can control all the mining infrastructure and preclude entry. While the blockchain protocol provides some security guarantees even when there is a single miner, a single miner will be able to set a minimal transaction fee because the single miner can ensure that any transaction that offers a lower fee will not be processed. The single miner can preclude entry of small miners if it maintains the reward per computational unit strictly below c_m and can make positive profits if his own cost is lower than c_m.

Our analysis presents a stylized view of miners, thereby abstracting from various real-world issues. Actual miners incur fixed costs to purchase mining equipment; available equipment is heterogeneous in price, quality, and vintage; innovative equipment manufacturers are also miners; electricity costs are location- and possibly miner-dependent. Future work will take up these nuances.

4.2. *User behaviour and equilibrium transaction fees*

We now characterize user behaviour in step (iii). The analysis in Section 4.1 shows that all miners, small and large, choose the block assembly policy A^*. The remainder of the article maintains that miners follow this behaviour and characterizes the induced subgame for users. In this context, the term equilibrium means the subgame perfect equilibrium behaviour of users in the subgame induced by all miners choosing A^*, *i.e.*, each block processes the K pending transactions which offer the highest transaction fees. The number of miners does not affect μ, the rate at which blocks are generated, or K, the block size, and therefore the number of miners does not affect users' choice of transaction fees.

From a user's perspective, the higher the fee he offers, the more likely the transaction will be included in an earlier block. Consider an equilibrium where all potential users participate and post their transactions in the system, with $G(\cdot)$ denoting the cumulative distribution function of the chosen transaction fees. A user i with delay cost c_i and WTP R_i who decides to post a transaction chooses his transaction fee b to maximize his net reward

$$R_i - b - c_i \cdot W(b \mid G), \tag{5}$$

with $W(b \mid G) = W\left(b \mid G, 1, \eta^*\right)$ denoting the equilibrium expected delay given transaction fee b and the CDF G. For brevity, we omit the dependence on the distribution of block assembly policies, as we maintain that all miners adopt the block assembly policy A^*. The following lemma characterizes the equilibrium expected delay.

Lemma 1. *In any equilibrium in which all potential users participate, the expected delay for a user with delay cost c_i is*

$$\mu^{-1} W_K\left(\hat{\rho}(c_i)\right), \tag{6}$$

where $\hat{\rho}(c_i) = \lambda \bar{F}(c_i)/K\mu = \rho \cdot \bar{F}(c_i)$ is the effective load from transaction with higher delay cost, and the function $W_K(\cdot)$ gives the expected number of blocks that pass until the transaction is processed.

The function $W_K(\cdot)$ is specified in Supplementary Appendix F.1. In particular, $W_K(0) = 1$ and $W_K'\left(\hat{\rho}\right) \geq 0$ for $\hat{\rho} \in [0, 1)$.

The intuition for Lemma 1 is as follows. Users face a queuing game where higher transaction fees imply higher processing priority. Standard arguments (see Hassin and Haviv (2003)) imply that users with higher delay cost will pay higher transaction fees and receive higher priority, and

therefore the arrival rate of transactions with higher priority is $\lambda \cdot \bar{F}(c)$. Analysis of the stochastic system shows that the number of blocks that pass until a transaction is processed depends only on the block size K and the effective load from higher priority transactions $\hat{\rho}(c_i) = \lambda \bar{F}(c_i)/K\mu$. Although $\rho < 1$ implies the system has sufficient capacity to process all transactions on average, the randomness of the arrival times implies the possibility of backlogs. The expression (6) captures the expected wait from such cases. Finally, the term μ^{-1} in (6) enables the statement of the result in terms of calendar time rather than the number of blocks. The particular function $W_K(\cdot)$ endogenously arises by the incentives set in the protocol. Supplementary Appendix E provides a plot of $W_K(\cdot)$.

Users' individual optimization implies:

Proposition 3. *Assuming that all potential users participate, there is a unique equilibrium. In it, a user with waiting cost $c_i \in [0, \bar{c}]$ chooses to pay a transaction fee $b(c_i)$, given by*

$$b(c_i) = \rho \int_0^{c_i} f(c) \cdot c \cdot \mu^{-1} W_K'\left(\rho \bar{F}(c)\right) dc. \tag{7}$$

These transaction fees coincide with the payments that result from selling priority of service in a VCG auction.

The net reward for a user with delay cost c_i and WTP R_i is

$$u(R_i, c_i) = R_i - \mu^{-1} \int_0^{c_i} W_K\left(\rho \bar{F}(c)\right) dc. \tag{8}$$

The Bitcoin protocol indirectly entails a priority auction, although no auctioneer is present. Users with higher waiting costs pay higher transaction fees and wait less. Users' bids have the VCG property that each user bids an amount equal to the externality he imposes on others by delaying their transactions. Equation (8) implies that users with lower delay cost c_i bear lower total costs (total of paid fees and delay costs). This is due to information rents. The highest costs are born by users with $c_i = \bar{c}$ and are equal to $\bar{R} = \mu^{-1} \int_0^{\bar{c}} W_K\left(\rho \bar{F}(c)\right) dc$.

The equilibrium allocation of priority is efficient. However, the allocation of delay takes the particular form because of the blockchain design. A different design or increased values of μ, K can reduce waiting costs for all transactions. Note that transaction fees depend on ρ and therefore will change with changes in λ, μ, K.

Finally, we verify that all potential users prefer to participate under the assumption that WTP is sufficiently high given the load ρ.

Lemma 2. Let $\bar{R} = \mu^{-1} \int_0^{\bar{c}} W_K\left(\rho \bar{F}(c)\right) dc$. If $R_H \geq R_L > \bar{R}$, there is a unique equilibrium where all potential users participate. In equilibrium, all users receive strictly positive net reward.

Thus, equilibrium behaviour of users does not depend on their WTP R, assuming that it is sufficiently high. All users participate regardless of their WTP, and the transaction fees paid are independent of WTP. Each user pays a fee equal to the externality he imposes on other users, and since all transactions are eventually processed, the externality involves only delays to other transactions.

Transaction fees under the firm and the BPS depend on different parameters. The firm sets prices based on user WTP, and transactions that do not pay the required fee are not processed.

Under the BPS, prices are determined in equilibrium based on user delay costs. All transactions are processed regardless of the fees they offer. Some users offer higher fees to reduce delays. Transactions which offer lower or zero fees are processed with greater delays. The BPS transaction fees depend only on the parameters K, μ, ρ, and the distribution of delay costs F. The transaction fees are nominally denominated in the system's native currency, but their value in USD is independent of the exchange rate e.

We summarize these results in the following theorem.

Theorem 2. *Let* $\rho = \lambda/\mu K \in (0,1)$ *and assume that*

$$R_H \geq R_L > \bar{R} = \mu^{-1} \int_0^{\bar{c}} W_K\left(\rho \bar{F}(c)\right) dc. \tag{9}$$

There is a unique equilibrium where all potential users participate and receive strictly positive surplus. Equilibrium transaction fees paid by users are independent of user WTP R_H, R_L*, and of the exchange rate* e*.*

Despite having excess capacity (i.e. $\rho < 1$*), the system raises strictly positive revenue from transaction fees.*

As seen in Section 3, a profit-maximizing firm will raise prices until some users receive no net benefit. The possibility that all users are net beneficiaries of the system distinguishes its service from a similar service provided by a profit-maximizing firm.

Another distinguishing feature of the system is its commitment to congestion pricing, a commitment that is difficult to modify even when circumstances change. Thus, the users are protected from being held up should they get locked into the BPS: if users lose their alternative payment methods then their WTP for the system goes up, but because transaction fees are independent of the WTP R (given that R_H, R_L are sufficiently high), users are protected from price increases. In contrast, users should be wary of getting locked into a conventional payment system, as a firm would raise prices should its users lose their alternative options (Grossman and Hart, 1986).

We highlight this as the following corollary.

Corollary 2. *Assume that the conditions of Theorem 2 are satisfied. Then, an increase in WTP* R *does not change equilibrium transaction fees.*

Corollary 2 may appear as good news to users. However, the pricing level depends on the congestion in the system $\rho = \lambda/\mu K$ and may be inefficient.

4.3. *Determination of infrastructure level and welfare*

Building on the two preceding subsections, this subsection shows the total revenue from transaction fees and the system's level of infrastructure. Moreover, it calculates the welfare level associated with the BPS and compares it to that delivered by a profit-maximizing firm. The following considers the equilibrium characterized by Theorems 1 and 2, and assumes the conditions of Theorem 2 are satisfied.

Aggregating (7) over all users delivers

Theorem 3. *Total revenue from transaction fees per unit time is*

$$\mathrm{Rev}_K(\rho) = K\rho^2 \int_0^{\bar{c}} cf(c)\bar{F}(c)W_K'\left(\rho\bar{F}(c)\right)dc. \tag{10}$$

Equation (10) complements equation (2) to determine the network's computational power in equilibrium. Equation (10) shows that total revenue from transaction fees depends only on K, ρ, and the distribution of delay costs F. It implies that the revenue depends on μ and λ only through $\rho = \lambda/\mu K$. Thus, holding the type distribution function F fixed, a system with double the demand λ and double the block rate μ will raise the same amount of revenue as the original system but will have twice as many users, each of whom will pay half the transaction fee paid by the corresponding user in the original system.

Note that there is no guarantee that the equilibrium number of miners is adequate for the system's reliability and security. The protocol can dictate the amount of newly minted coins S that are awarded to miners, but the exchange rate e may fluctuate during the life of the system. The revenue from transaction fees does not depend on the exchange rate but varies with the congestion ρ which is a function of the predetermined parameters μ, K as well as the potential demand λ that may change over time. Moreover, a shortage of mining resources does not lead to higher fees or a more favourable exchange rate; if anything, it is likely to result in the opposite. On the other hand, an abundance of mining resources does not lead to lower fees or a less favourable exchange rate. The equilibrium analysis is applicable if user WTP for the system R_H, R_L are sufficiently high given the equilibrium number of miners N.

Next, we calculate welfare by accounting for the total benefits and costs of the system. Since all users are served, the system generates $\lambda_H R_H + \lambda_L R_L$ for users per unit time. The users pay transaction fees and incur delay costs. All miners receive a reward equal to c_m per mining unit. Marginal miners whose cost is c_m will therefore break even and spend all the revenue they receive on operating costs.

Theorem 4. *If all miners have a cost c_m per computational unit and no new coins are minted*[18] *then welfare is given by*

$$\lambda_H R_H + \lambda_L R_L - \mathrm{DelayCost}_K(\rho) - c_m \cdot N, \tag{11}$$

where the total delay costs incurred by users is

$$\mathrm{DelayCost}_K(\rho) = K\rho \int_0^{\bar{c}} cf(c)\, W_K\left(\rho\bar{F}(c)\right)dc. \tag{12}$$

Miners break even and spend all the revenue they receive on operating costs.

The total benefit from processing transactions is $\lambda_H R_H + \lambda_L R_L$, as all transactions are processed. The cost $c_m \cdot N$ is the cost of server infrastructure, where competition between the miners ensures that infrastructure is provided at cost c_m and miners make no profit. The delay costs $\mathrm{DelayCost}_K(\rho)$ are necessary in order to raise revenue from users, as users have an incentive to pay higher transaction fees only if transactions with low fees suffer delays.

18. That is, $S = 0$, as will be the case for the BPS in the long run. Currently, the BPS funds most of its mining cost by minting new coins. The welfare calculations remain unchanged if the BPS can mint a finite amount of new coins and the opportunity cost of awarding the coins to miners is equal to its value. We defer determination of the welfare costs of minting new coins to future work.

If, in deviation from the theorem's assumption, some miners have an average cost lower than c_m, they make a profit. In such case, welfare will be higher by these miners' profit.

This allows us to compare the BPS and a conventional payment system that is run by a firm. Under our assumptions, the cost of operating the BPS is $c_m \cdot N$, while the cost of operating a firm-run payment system is $c_f \cdot \lambda_H$. It appears that it is more expensive to run the BPS because the decentralized protocol requires additional computational overhead. Moreover, if the BPS is successful and popular, the implied congestion can lead to an equilibrium value of N that is too high. The BPS also has the additional delay cost $\text{DelayCost}_K(\rho)$, while the firm processes transactions immediately. On the other hand, the BPS serves all potential demand, while under the firm there is a dead-weight loss because R_L users are not served, losing $\lambda_L \cdot R_L$ of potential generated value. Altogether, we get that if

$$\lambda_L R_L > c_m \cdot N - c_f \lambda_H + \text{DelayCost}_K(\rho) \tag{13}$$

welfare is higher under the BPS than under a firm. Note that the two sides of inequality (13) depend on different sets of parameters, and therefore the comparison can go either way. Essentially, the BPS allows society to pay for a more costly infrastructure on which competitive pricing is guaranteed, and that can be beneficial if dead-weight loss is substantial.

Beyond this calculations-based comparison, there are differences worth mentioning. For instance, a firm-run system operates under the legal system and can offer procedures to retrieve lost accounts and reverse erroneous or fraud-inspired payments. The BPS cannot offer such services but is transparent and does not require trust in any individual component.

5. PROTOCOL DESIGN FOR EFFICIENT CONGESTION PRICING

The following corollary of Section 4 motivates this section's main question, namely how to set the system's parameters K and μ in response to λ in order to achieve desired combinations of fee revenue and delays.

Corollary 3. In equilibrium, if $\rho = 0$, both delay cost and revenue are zero. For any fixed K, both revenue (and with it, infrastructure provision by miners) and delay cost are strictly increasing in ρ.

Figure 2 shows how revenue from transaction fees and delay cost vary with ρ under the parameters $K = 2,000$ and $c \sim U[0,1]$. The figure assumes that all agents participate, and therefore revenue tends to infinity as $\rho \to 1$. When agents choose whether to participate, revenue will be bounded, as agents may not participate as the system gets congested (see Supplementary Appendix B). The figure looks similar for other distributions of delay costs (see Supplementary Appendix E for a plot of other distributions).

The current Bitcoin protocol uses fixed capacity parameters K and μ, and therefore the congestion ρ varies with demand. This is undesirable, as the amount of revenue generated can be too high or too low relative to the desired levels of reliability and security. An alternative design should adjust K, μ to accommodate demand variations and thereby maintain desirable levels of congestion and revenue.

While our focus is on the economic aspects of the design, we note that designing such a decentralized protocol raises engineering challenges. First, the protocol must maintain agreement on K, μ among the independently operating miners. Thus, the parameter adjustment rule must be encoded in the protocol and use only information shared among all miners. If $\rho < 1$, a rule that uses the volume of recently processed transaction as a proxy for demand can dynamically adjust

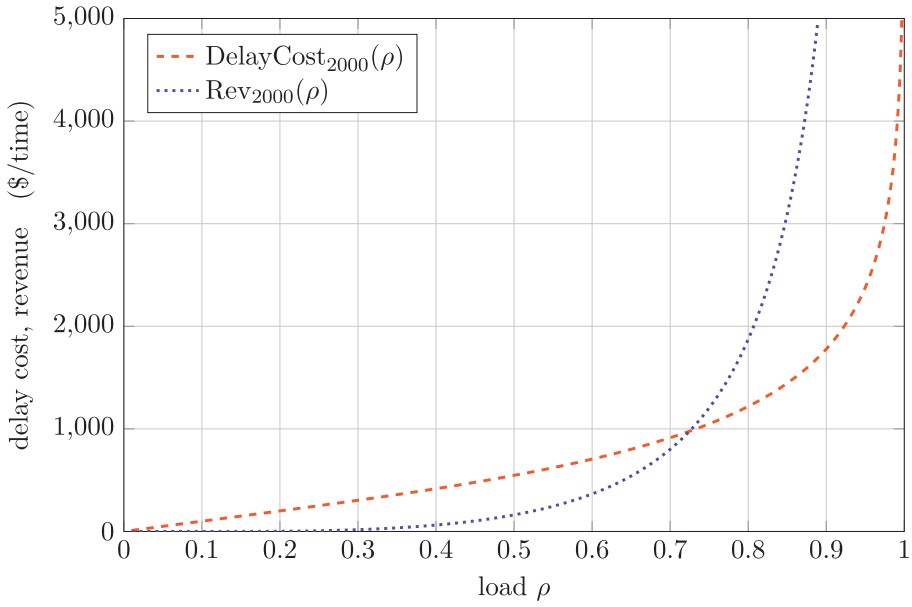

FIGURE 2

Revenue and delay cost for varying congestion level ρ. Delay costs are distributed according to $c \sim U[0,1]$ and the block size is $K = 2,000$.

K, μ and maintain agreement on them.[19] Second, the consensus protocol may constrain K, μ. The Nakamoto consensus protocol requires that block inter-arrival times are sufficiently large relative to the network lag given the block size.[20] New designs may allow a larger range of parameters.[21] In the analysis below, we determine the ideal K, μ from an economic perspective. Addressing the engineering limitations is left for future work. Our suggestion can guide the choice of K, μ within the feasible range.

The choice of K, μ should achieve the target revenue from transaction fees and should minimize the delay costs imposed on users. Note that by an appropriate choice of K, μ in response to demand λ, we can achieve the desired ρ and desired revenue from transaction fees in USD, regardless of exchange rate fluctuations. Although transaction fees are denominated in bitcoin, their USD value reflects the USD value of shortening delays. The protocol obtains the USD market value of delay reduction without the need to learn the exchange rate.

19. Such a rule can be implemented by modifying the adjustment of the hash difficulty (as explained in Appendix A). Currently, the difficulty adjusts in accordance with the total computing power of the network to maintain average block mining frequency of 10 min. Our suggested alternative design can similarly adjust the difficulty to maintain that on average a fraction ρ of blocks is used.

20. Croman *et al.* (2016) studies the limitations of the computer network operating the BPS. Pass *et al.* (2017) provides theoretical bounds for block rate in the Nakamoto consensus.

21. Bitcoin's capacity limitations led to many suggestions of alternative protocols. For example, Sompolinsky and Zohar (2015) suggest the GHOST protocol in which blocks form a tree (instead of a chain); Gilad *et al.* (2017) and Bentov *et al.* (2016) suggest alternative proof of stake protocols. Many of these suggested protocols maintain the main features of our model (in particular, batch processing of transactions), and can incorporate similar congestion pricing mechanisms.

Raising revenue from transaction fees requires positive ρ and therefore delay costs. To better understand the dependency on K, μ, and the implied trade-offs between revenue and delay costs, we provide the following simplified approximate expressions.

Lemma 3. For any $\hat{\rho} \in [0,1)$ we have that[22]

$$\lim_{K\to\infty} W_K(\hat{\rho}) = W_\infty(\hat{\rho}) = 1 + \frac{1}{\rho}e^{-1/\rho} + o\left(\frac{1}{\rho}e^{-1/\rho}\right)$$

where the function $W_\infty : [0,1) \to [1,\infty)$ is explicitly given in Appendix F.4. Moreover, $W_\infty(0) = 1, W'_\infty(0) = 0$ and $W'_\infty(\hat{\rho}) > 0$ for $\hat{\rho} \in (0,1)$.

A given transaction with $\hat{\rho} \in [0,1)$ will be processed within $W_K(\hat{\rho})$ blocks on average. We have that $1 \leq W_K(\hat{\rho}) < \infty$ because the inclusion of a transaction in a block depends both on how many pending transactions have accumulated at the time the block is generated as well as how the priority of the given transaction ranks among the accumulated transactions. The former is random due to the random time between blocks, and the latter is random due to the random arrival of transactions. When blocks are fairly large, there is still randomness due to their random arrival time, but the arrival of higher priority transactions does not create much additional randomness.[23] As a result, $W_K(\hat{\rho})$ is almost independent of K for large K. Calculations show that the approximation already appears good for $K = 20$; with Bitcoin's $K = 2000$ we can comfortably use this approximation. For additional intuition and the proof of Lemma 3, see Supplementary Appendix F.4.

Using Lemma 3, we can give the following simplified expressions for revenue and delay costs.

Theorem 5. *For a fixed-load $\rho \in [0,1)$, as the block size $K \to \infty$, we have that*[24]

$$\mathrm{Rev}_K(\rho) = K \cdot \mathrm{Rev}_\infty(\rho) + o(K),$$
$$\mathrm{DelayCost}_K(\rho) = K \cdot \mathrm{DelayCost}_\infty(\rho) + o(K),$$

22. Given arbitrary functions $f(\cdot)$ and $g(\cdot)$ and a positive function $h(\cdot)$, as $\rho \to 0$, we will say that $f(\rho) = g(\rho) + O(h(\rho))$ if $\limsup_{\rho\to 0} |f(\rho) - g(\rho)|/h(\rho) < \infty$, *i.e.*, if the difference between f and g is asymptotically bounded above by *some* constant multiple of h. Similarly, we will say that $f(\rho) = g(\rho) + o(h(\rho))$ if $\limsup_{\rho\to 0} |f(\rho) - g(\rho)|/h(\rho) = 0$, *i.e.*, if the difference between f and g is asymptotically dominated by *every* constant multiple of h.

23. To gain intuition, consider a user i with delay costs c_i that posts a transaction at time t_0 when there are no pending transactions. The following block arrives after some random time $t \cdot \mu^{-1}$, where $t \sim Exp(1)$. The probability that i's transaction is included in the following block is the probability that, between t_0 and $t_0 + t \cdot \mu^{-1}$, less than K higher priority transactions arrive. The number of higher priority transactions given t has distribution $X_t \sim \mathrm{Poisson}(\lambda \bar{F}(c_i) \cdot t\mu^{-1}) = \mathrm{Poisson}(t \cdot K\hat{\rho})$. The realized number is random because t is random and also because the number of arrivals given t, X_t, is random. However, the variance of X_t is of order K, and therefore, as $K \to \infty$, the number of arrivals given t measured in block equivalents, X_t/K, can be well approximated by its expectation $t\hat{\rho}$. Thus, the probability that the transaction will be included in the next block converges according to $\mathsf{P}(X_t < K) \to \mathsf{P}(t < \hat{\rho}^{-1})$, which only depends on $\hat{\rho}$.

24. Given arbitrary sequences $\{f_K\}$ and $\{g_K\}$, and a positive sequence $\{h_K\}$, as $K \to \infty$, we will say that $f_K = g_K + o(h_K)$ if $\limsup_{K\to\infty} |f_K - g_K|/h_K = 0$, *i.e.*, if the difference between f and g is asymptotically dominated by *every* constant multiple of h. Similarly, we will say that $f_K = g_K + \Omega(h_K)$ if $\liminf_{K\to\infty} |f_K - g_K|/h_K > 0$, *i.e.*, if the difference between f and g is asymptotically bounded below by *some* constant multiple of h.

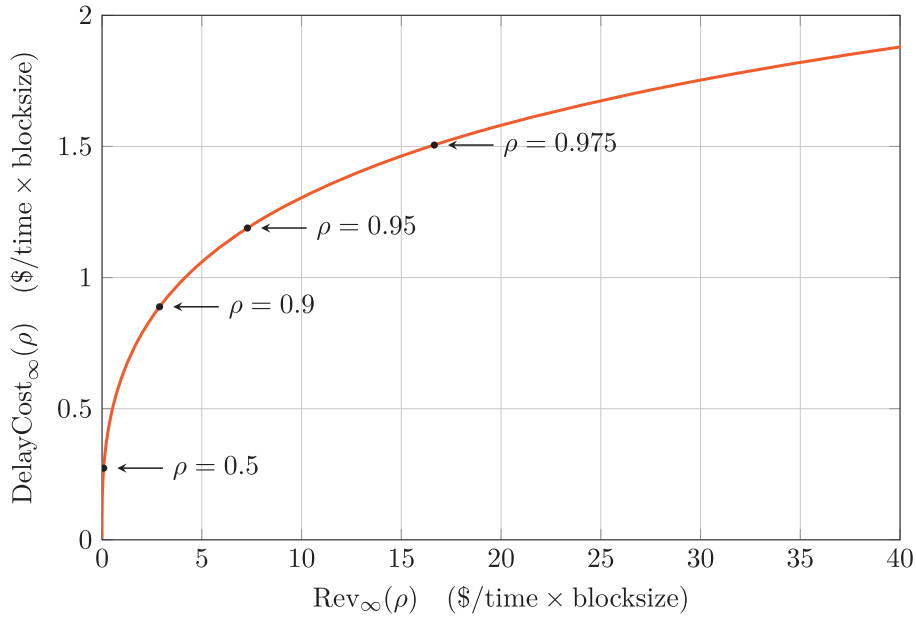

FIGURE 3

The parametric curve $\left(\text{Rev}_\infty(\rho), \text{DelayCost}_\infty(\rho)\right)$ for $\rho \in [0,1)$, describing (up to a scaling by blocksize) the achievable combinations of revenue and delay cost for systems with large blocksize. The distribution of delay costs is taken to be $c \sim U[0,1]$.

where

$$\text{Rev}_\infty(\rho) \triangleq \rho \int_0^{\bar{c}} \left(\bar{F}(c) - cf(c)\right) W_\infty\left(\rho \bar{F}(c)\right) dc,$$

$$\text{DelayCost}_\infty(\rho) \triangleq \rho \int_0^{\bar{c}} cf(c) W_\infty\left(\rho \bar{F}(c)\right) dc.$$

Theorem 5 offers simple approximations of the dependencies of revenue and delay costs on K. The expressions $\text{Rev}_\infty(\rho), \text{DelayCost}_\infty(\rho)$ are functions of only ρ and F. To a good approximation, the dependency of $\text{Rev}_K(\rho), \text{DelayCost}_K(\rho)$ on K is only through a scaling factor of both of these expressions. See Supplementary Appendix E for plots showing the goodness of approximation.

Note that Theorem 5 critically relies on the randomness of block inter-arrival times. If $\rho < 1$ and blocks were to arrive at deterministic fixed time intervals (say, exactly every 10 min), then for large K every pending transaction would be processed in the next block. Hence users would not have incentive to pay any transaction fees. The random arrival of blocks allows the system with large blocks to generate revenue even when $\rho < 1$.

Figure 3 plots how the pairs $\left(\text{Rev}_\infty(\rho), \text{DelayCost}_\infty(\rho)\right)$ vary with ρ, assuming the distribution of delay costs is $c \sim U[0,1]$. From Theorem 5, the pairs $\left(\text{Rev}_K(\rho), \text{DelayCost}_K(\rho)\right)$, for any fixed K and varying ρ, are scaled versions of the depicted curve. Thus, the curve informs us of the delay costs that are necessary for raising a given amount of revenue for any K.

The figure shows that a significant amount of delay cost is necessary to raise even a small amount of revenue. We formally show this in Theorem 6.

Theorem 6. *For any F, as $\rho \to 0$, we have that*

$$\mathrm{Rev}_\infty(\rho) = O\left(e^{-1/\rho}\right),$$
$$\mathrm{DelayCost}_\infty(\rho) = \rho \cdot \mathbb{E}[c] + o(\rho).$$

In other words, for small values of the load ρ, the delay cost grows linearly but the revenue grows more slowly than any polynomial.

The intuition is as follows. For $\rho \approx 0$, all transactions are likely to be processed in the next block regardless of their priority because the block is unlikely to reach its maximal size. In contrast, total delay costs scale linearly, as every transaction needs to wait for at least one block and higher ρ implies more waiting. Therefore, as the load increases from $\rho \approx 0$, both revenue and delay costs increase but delay costs grow more than exponentially faster than revenue.

Together with Theorem 5, this implies that using a larger K to raise a desired level of revenue R^* will yield unfavourable results. We formally state this as the following theorem.

Theorem 7. *Consider a desired level of revenue $R^* > 0$ and a block size K. Define $\mathrm{DelayCost}^*_K(R^*)$ to be the delay cost required to achieve revenue R^* under the approximation for large K, i.e.,*

$$\mathrm{DelayCost}^*_K(R^*) \triangleq K\,\mathrm{DelayCost}_\infty\left(\mathrm{Rev}^{-1}_\infty(R^*/K)\right),$$

with $\mathrm{Rev}^{-1}_\infty(R^*) \triangleq \inf\left\{\rho > 0 \,:\, \mathrm{Rev}_\infty(\rho) \geq R^*\right\}$ being the minimal load required to achieve revenue R^*.

Then,

$$\mathrm{DelayCost}^*_K(R^*) = \Omega\left(\frac{K}{\log K}\right).$$

Figure 4 illustrates the possible attainable values for revenue and delay given different values of K and ρ, assuming delay costs are distributed uniformly in $[0, 1]$. Each curve shows the attainable values for revenue and delay for a fixed value of K and a range of possible ρ. The plot shows that a lower value of K allows raising any level of revenue at a lower delay cost to users.

Each curve's two main features are (1) monotonicity, *i.e.*, longer delays are required to generate more revenue and (2) the curve is asymptotically vertical at the origin, *i.e.*, to move from zero to some revenue, the delay cost has to be substantial. These insights transcend the specific $U[0, 1]$ distribution of c underlying the figure. However, note that these calculations ignore technological constraints and assume that no users opt out of the system. All curves are approximately a scaled version of the curve in Figure 3 (note the logarithmic scale for the vertical axis), as implied by Theorem 5.

To summarize, this analysis suggests the following simple adaptations to the current protocol. First, a smaller block size K is preferable. Second, an adjustment of the block rate to $\mu = \lambda / (K\rho^*)$ in response to demand λ. This keeps congestion constant at ρ^*, yielding a stable, desired level of revenue.[25]

25. Clearly, there are communication and other limitations that limit the range of feasible μ and K. This article ignores these engineering challenges.

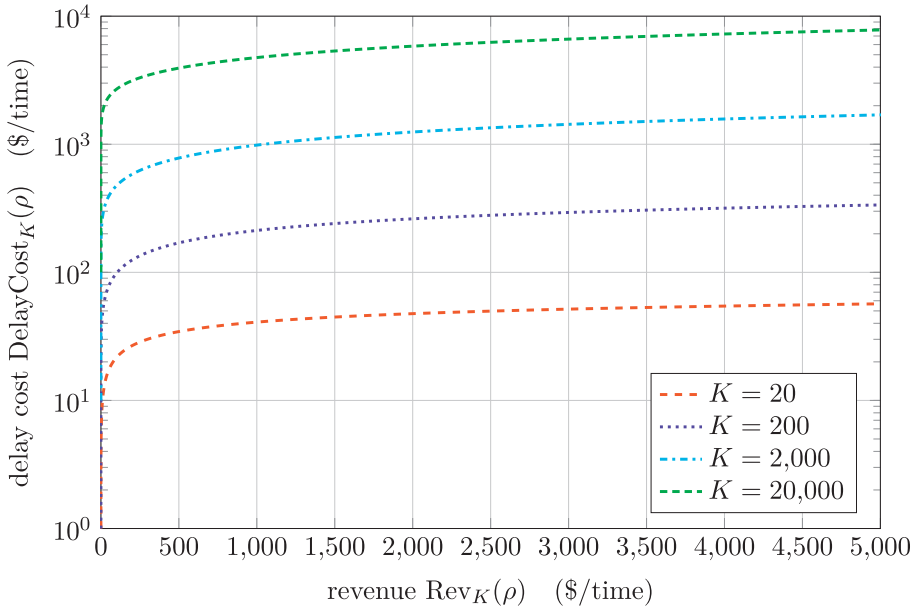

FIGURE 4

Possible pairs of revenue and delay cost as ρ varies, for different values of K, where delay costs are distributed according to $c \sim U[0,1]$.

6. DATA

6.1. *Mining profitability*

We compare our results to empirical estimates given by Croman *et al.* (2016), who estimate that the total expenditure of miners during October 2015 was approximately 5,840 USD per block. Croman *et al.* (2016) attribute the vast majority of the cost to the costs of electricity and hardware used in the attempts to get selected to mine the next block. During that period, the mining reward per block was 25 bitcoins plus negligible transaction fees, or approximately 6,000–7,500 USD (the bitcoin-USD exchange rate fluctuated during the month). This back of the envelope calculation suggests that miners who buy electricity at market prices approximately break even, which is consistent with our analysis. Websites that offer information to potential miners about mining profitability of various cryptocurrencies[26] give advice that is consistent with this observation. Furthermore, while some groups controlled a significant fraction of the computational power in the network, there is no evidence that even large miners tried to influence fee levels.

6.2. *The relation between congestion and transaction fees*

Average block size in MB can be used as a measure of the actual congestion in the BPS. In practice, the BPS limited blocks to 1MB of data per block until 21st August 2017. This corresponds to approximately $K = 2{,}000$ transactions per block. In our model, the congestion parameter ρ is equal to the average number of transactions per block divided by K. Analogously, we interpret the average size of a block relative to the 1MB limit as a proxy for congestion ρ. Each point in

26. https://www.coinwarz.com/cryptocurrency/, retrieved 20 June 2017.

Figure 1 corresponds to one day in the BPS, displaying daily average transaction fees per block and daily average block size.[27] The plot also includes a solid line generated by our model as follows. We set $K=2,000$, and normalize time so that a time unit is 10 minutes and set $\mu=1$. The distribution of users' delay cost is unknown and arbitrarily set to $F=U[0,\bar{c}]$ with $\bar{c}=0.1$ USD/10 min. The resulting total revenue per unit time $\text{Rev}_{2000}(\cdot)$ is the expected total transaction fees per block, which is displayed by the solid black line in Figure 1.

Note that the solid line produced by our model matches the broad patterns in the data. Figure 1 shows that transaction fees are negligible when congestion is low. Transaction fees become substantial when congestion reaches 80%. Transaction fees increase rapidly as congestion approaches 1, even though the system has excess capacity.

7. CONCLUSION

Bitcoin presents a computer science breakthrough, showing the feasibility of a decentralized payment system that relies on a collection of unrelated parties without the need for a central intermediary. This article shows that Bitcoin also provides an economic innovation that can address concerns of the harm of monopoly power of platforms. The BPS shows the feasibility of a decentralized platform in which users are protected from the harms of monopoly pricing, even if users have no alternative to the platform. The platform can fund itself by user fees that are determined in a market equilibrium. Competition and free entry among the service providers renders all participants to be price takers.

Critical ingredients of our analysis are costly effort on the part of miners combined with free entry and exit. Our results can be extended to other protocols, *e.g.*, Proof of Stake, should they retain these ingredients. Issues left unaddressed in this paper include engineering challenges limiting the scale at which a decentralized system can operate; ensuring the security of the system against attacks; determination of the coin's exchange rate and its volatility.

A comprehensive comparison between the BPS and a traditional payment system operated by a profit-maximizing firm requires consideration of multiple attributes, many of which are outside the scope of this article's analysis. As opposed to traditional systems, the BPS does not require trust in any entity. On the other hand, the BPS cannot provide some services: for instance, transactions cannot be reversed in case of error or fraud, and users who lose the credentials to their accounts cannot retrieve their balances.

We think of the BPS as a blueprint showing the feasibility of a decentralized design. The BPS demonstrates the power of competition and free entry of service providers within a platform. Future work is likely to improve upon these insights and apply them in other domains.

Since service provision requires resource expenditure, the operation of a decentralized platform necessitates a means to transfer value from users to service providers. The BPS allows such value transfers under the assumption that balances within its system (denominated in the system's native coin, bitcoin) are valuable. Determination of this value is left for future work.

Another feature that sets Bitcoin apart is that a protocol, rather than a managing organization, runs Bitcoin. Unlike a managing organization, a protocol lacks an easily workable mechanism to change prices, offerings, and rules, implying the stability of these attributes. Such stability can be considered an asset or a liability of the system.

27. Transaction fee and block size data is from http://blockchain.info, and the number of blocks per day is from https://data.bitcoinity.org. Each point is a daily average over the interval 1 April 2011–30 June 2017. The starting date 1 April 2011 was selected as this is roughly when the fees per block started exceeding 1 USD. The end date does not extend to present day because the BPS changed the method for calculating a block's size in August 2017.

The blockchain protocol presents a novel economic design that would merit an economist's attention and scrutiny even if it had not been functional. Currently, the BPS handles daily transactions worth several billion dollars in aggregate. It can serve as a compelling proof of concept that should further encourage economists to study this marvellous structure and its future descendants.

Acknowledgments. This article was originally circulated in August 2017 and has also appeared with the title "An Economic Analysis of the Bitcoin Payment System." We are grateful to Eric Budish, Alex Frankel, Campbell Harvey, Refael Hassin, Hanna Halaburda, Tammuz Huberman, Emir Kamenica, Seth Stephens-Davidowitz, Jessica Mantel, Canice Prendergast, Bernard Salanie, Ran Snitkovsky, Aviv Zohar, Adam Szeidl (the editor) and the referees for helpful conversations and suggestions, and seminar participants at the Central Bank of Finland, Columbia, EIEF, MSR-NYC, Northwestern, NY Computational Economics, NYU, NYU-IO day, Tel Aviv University, Central Bank of Italy, LUISS, University of Turin, Bocconi, the Paul Woolley Conference, the CEPR conference on Money in the Digital Age, and Stanford for helpful comments. The authors advise FinTech companies. This work is supported by the Robert H. Topel Faculty Research Fund at the University of Chicago Booth School of Business.

Supplementary Data

Supplementary data are available at *Review of Economic Studies* online. And the replication packages are available at https://doi.org/10.5281/zenodo.4502715.

Data Availability Statement: The data used in this paper is available on Zenodo at https://doi.org/10.5281/zenodo.4502715.

A. A BRIEF DESCRIPTION OF THE BITCOIN PAYMENT SYSTEM

This appendix provides a simplified explanation of the permissionless blockchain protocol that underlies the Bitcoin Payment System and is the basis of many other cryptocurrencies. The description focuses on the economic elements.[28] In order to describe what the Bitcoin system does, it is useful to first explain what is needed for a payment system, such as PayPal or FedWire, or the maintenance of electronic balances in a modern bank.

An electronic payment system functions as a record (or a ledger) of accounts. Each account is associated with a user and his balance. It allows users to check their balances, and it allows a user to debit his balance and credit the debited amount to another account. Only an account owner can debit the account. Balances do not change without a legal transfer, *i.e.*, a transfer that conforms to the system's stated rules.

One simple implementation is just a spreadsheet (or another bookkeeping device) that only a trusted authority can modify. Allowing multiple computers to maintain and update the ledger requires a more elaborate structure. This distributed ledger structure requires synchronization across the servers but is, in principle, more robust than a single server system. Maintaining consensus in a distributed computer system has been known to be straightforward as long as the computers are trusted (see Tanenbaum and Van Steen (2007)).

The Bitcoin system is designed for an environment which lacks a trusted authority. Therefore, its ledger must be maintained and updated by a collection of computer servers, called miners, none of which are trusted. They are assumed to be selfish, *i.e.*, to respond to incentives in a profit-maximizing way. Moreover, they offer or withdraw their services according to profit opportunities they perceive.

Although legal transactions are processed by untrusted miners, the system as a whole is secure, *i.e.*, it processes all legal transactions and no other transactions. The collection of miners jointly holds a single ledger, meaning that there must be consensus among miners about current balances. Moreover, consensus must be maintained as balances change.

Bitcoin's ledger is a public database called blockchain, which can be verified by third parties through cryptography. The system arranges for the miners to be compensated for their services in such a way that when each of them maximizes his profit and believes that other miners similarly maximize their profits, the system has the properties sketched above.

Initially, all balances are at zero. Over time, the protocol mints new coins which it adds to the balances of successful miners. The system holds the record of all balance changes. The manifestation of a transaction is a message which a sending account transmits to all the miners. It states the sending account, receiving account, amount transferred, transaction fee, and cryptographic signature by the sending account. A transaction is processed by adding the appropriate message to the

28. In particular, this description omits discussion of potential attacks on the system. For further details and an explanation of the cryptographic elements of the system, please refer to Narayanan *et al.* (2016).

end of the ledger. The cryptographic signature allows any third party to verify that the transaction was indeed authorized by the holder of the sending account. Since the ledger is public, any third party can verify that the sender indeed held a balance sufficient for the transfer.

The public ledger is saved in the distributed blockchain format, in which the transaction data are partitioned into a sequence of blocks. These blocks are periodic updates to the ledger. Notably, the ledger does not update instantly following the appearance of a new transaction. Rather, it updates on average every ten minutes with a block summarizing a subset of the recent pending transactions which had not been included in a previous block. Remaining unprocessed transactions wait to be processed in future blocks. As of July 2017, the maximal block size is 1MB.[29]

New transactions are processed when they are included in a block that is added to the ledger, which happens as follows. Each miner holds a copy of the current ledger *i.e.*, all previous blocks. All transaction requests are broadcast to all miners. The set of pending transactions that reaches each miner may vary slightly across miners due to network imperfections, rendering non-trivial the choice of a universally agreed upon record of transactions. To ensure that Bitcoin maintains a unique record of transactions, a single miner is selected to add a block of transactions to the ledger. Since there is no trusted authority to make the selection, a tournament is used to randomly select a winning miner. To participate in the tournament, miners exert effort[30] (known as proof of work) that is useful only for generating a verifiable random selection of a miner without the need of a trusted randomization device.

Periodically (currently approximately every 10 minutes), the tournament randomly selects one miner as the winner, assigning his block as the next in the chain, thereby making that block a mined block. The mined block is transmitted to all the other miners, who verify the legality of that block and vet all transactions included in the block. Miners add a newly mined legal block to their copy of the ledger and proceed to add new blocks on top of it. Miners ignore mined blocks that are not legal.

The tournament-winning miner is paid a reward when he mines a new block but can withdraw his reward only after newer blocks augment the chain on top of his block. Other miners will build on top of his block only if they consider it legal. Hence, the incentive is to assemble and create legal blocks. Consensus forms on a ledger that includes the new block. The process continues in the same manner for the following ten minutes (on average) and so on.[31]

The miner that created a block is paid from two sources. One consists of newly minted coins, the exact number of which is protocol-determined and is decreasing with time. (Crediting successful miners with newly minted coins moves the system early on from having zero balances to having positive ones.) The second consists of the fees offered by the transactions in the mined block. This second source is the focus of the article.

This system will have the following desired properties. All miners are synchronized to hold the same ledger of processed transactions. No single miner controls the system, because every 10 min the ability to process transactions is given to a randomly chosen miner. Balances change only with a legal transaction because any transaction that is added is vetted by other miners to be valid, and transactions cannot be deleted from the ledger.

29. As of July 2017, the protocol limits each block to 1MB of data to ensure each block can be transmitted promptly throughout the network. This limits each block to no more than approximately 2,000 transactions, as the average transaction uses 0.5 KB of data (Zohar 2015).

30. The tournament selects a random winner without the need of a trusted authority through use of a hash function. The hash function is a deterministic one-way function that produces a hash value, interpreted as a pseudo-random real number between 0 and 1. A block is said to be a winning block if it is a legal block and its hash value is below a target value. A legal block contains, in addition to transaction data, an unrestricted "nonce" field for which the miner can input any numerical value. The cryptographic properties of the hash function imply that finding such a block requires a brute-force search, iterating over numerical values for the nonce and computing the hash value for each of them. Roughly speaking, each attempt for a value of the nonce generates an independent random draw of a hash value, distributed uniformly between 0 and 1.

To participate in the tournament, miners assemble their blocks and use their computational power to iterate over values of the nonce. Each attempt for a nonce value has an independent probability of generating a winning block, with probability equal to the target value. Because the target value is very small, a miner's chance to win the tournament within a time period is proportional to the number of nonce values attempted within the period. A miner with a winning block is said to "mine the block," and the winning block can be verified by any third party by recomputing the hash.

The target value adjusts over time so that a block is mined every 10 min (on average). For example, if the overall computational power of miners doubles, then the target value is halved and twice as many attempts (on average) are required to find a winning block.

31. There is a small probability that two or even more blocks are vying to be accepted as the newest block. This situation is called a fork. Bitcoin's convention calls for newer blocks to be built on top of the longest chain. This convention resolves forks. Eyal and Sirer (2014) analyse strategic issues between miners.

REFERENCES

ABADI, J. AND BRUNNERMEIER, M. (2018), "Blockchain Economics" (NBER Working Paper No. 25407).
ARNOSTI, N. AND WEINBERG, S. M. (2018), "Bitcoin: A Natural Oligopoly", in *10th Innovations in Theoretical Computer Science Conference (ITCS 2019)* (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik).
ATHEY, S., PARASHKEVOV, I., SARUKKAI, V. et al. (2016), "Bitcoin Pricing, Adoption, and Usage: Theory and Evidence" (Stanford University Graduate School of Business Research Paper No. 16-42).
BABAIOFF, M., DOBZINSKI, S., OREN, S. et al. (2012), "On Bitcoin and Red Balloons", in *Proceedings of the 13th ACM Conference on Electronic Commerce* (New York, NY: Association for Computing Machinery) 56–73.
BASU, S., EASLEY, D., O'HARA, M. AND SIRER, E. (2019), "Towards a Functional Fee Market for Cryptocurrencies", *Capital Markets: Market Microstructure Journal*, arXiv preprint arXiv:1901.06830 .
BENTOV, I., PASS, R. AND SHI, E. (2016), "Snow White: Provably Secure Proofs of Stake", *IACR Cryptology ePrint Archive,* **2016**, 919.
BIAIS, B., BISIERE, C., BOUVARD, M. et al. (2018), "The Blockchain Folk Theorem" (Swiss Finance Institute Research Paper No. 17-75).
BUDISH, E. (2018), "The Economic Limits of Bitcoin and the Blockchain" (NBER Working Paper No. 24717).
BUTERIN, V. (2018), "Blockchain Resource Pricing" https://ethresear.ch/uploads/default/original/2X/1/197884012ada193318b67c4b777441e4a1830f49.pdf.
CARLSTEN, M., KALODNER, H., WEINBERG, S. M. et al. (2016), "On the Instability of Bitcoin without the Block Reward", in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (New York, NY: Association for Computing Machinery) 154–167.
CATALINI, C. AND GANS, J. S. (2020), "Some Simple Economics of the Blockchain", *Communications of the ACM,* **63**, 80–90.
CHEN, X., PAPADIMITRIOU, C. AND ROUGHGARDEN, T. (2019) "An axiomatic approach to block rewards", in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies* 124–131.
CHIU, J. AND KOEPPL, T. (2017), "The Economics of Cryptocurrencies - Bitcoin and Beyond" (Working Paper).
CONG, L. W., HE, Z. AND LI, J. (2018), "Decentralized Mining in Centralized Pools" (George Mason University School of Business Research Paper No. 18-9).
CONG, L. W., LI, Y. AND WANG, N. (2018), "Tokenomics: Dynamic Adoption and Valuation" (Columbia Business School Research Paper No. 18-46).
CROMAN, K., DECKER, C., EYAL, I., et al. (2016), "On Scaling Decentralized Blockchains", in Kurt Rohloff, K., Clark, J., Meiklejohn, S., Wallach, D., Brenner, M., Ryan Eyal, P.Y.A. et al. (eds) *Proceedings of 3rd Workshop on Bitcoin and Blockchain Research* (Springer-Verlag).
EASLEY, D., O'HARA, M. AND BASU, S. (2017), "From Mining to Markets: The Evolution of Bitcoin Transaction Fees" (Working Paper).
EDELMAN, B. AND WRIGHT, J. (2015), "Price Coherence and Excessive Intermediation", *The Quarterly Journal of Economics* **130**, 1283–1328.
EVANS, D. S. AND SCHMALENSEE, R. (2005), *Paying with Plastic: The Digital Revolution in Buying and Borrowing* (Cambridge, MA: MIT Press).
EYAL, I., GENCER, A. E., SIRER, E. G. et al. (2016), "Bitcoin-ng: A Scalable Blockchain Protocol", in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, 45–59.
EYAL, I. AND SIRER, E. G. (2014), "Majority is Not Enough: Bitcoin Mining is Vulnerable", in *International Conference on Financial Cryptography and Data Security* (Springer) 436–454.
FELTEN, E. (2013), "Basic Economics of Bitcoin Mining" **URL:** *https://freedom-to-tinker.com/2013/02/05/basic-economics-of-bitcoin-mining/*
GANDAL, N. AND HALABURDA, H. (2014), "Competition in the Cryptocurrency Market" (CEPR Discussion Paper No. DP10157).
GANS, J. S. AND HALABURDA, H. (2015), "Some Economics of Private Digital Currency", in Goldfarb, A., Shane M Greenstein, S.M., and Tucker, C.E (eds) *Economic Analysis of the Digital Economy* (University of Chicago Press) 257–276.
GILAD, Y., HEMO, R., MICALI, S., et al. (2017), "Algorand: Scaling Byzantine Agreements for Cryptocurrencies", in *Proceedings of the 26th Symposium on Operating Systems Principles* (New York, NY: Association for Computing Machinery) 51–68.
GLAZER, A. AND HASSIN, R. (1986), "Stable Priority Purchasing in Queues", *Operations Research Letters,* **4**, 285–288.
GROSSMAN, S. J. AND HART, O. D. (1986), "The Costs and Benefits of Ownership: A Theory of Vertical and Lateral Integration", *Journal of Political Economy* **94**, 691–719.
HALABURDA, H. AND SARVARY, M. (2016), "Beyond Bitcoin", *The Economics of Digital Currencies* (US: Palgrave Macmillan).
HASSIN, R. (1995), "Decentralized Regulation of a Queue", *Management Science* **41**, 163–173.
HASSIN, R. (2016), *Rational Queueing* (Boca Raton, FL: CRC Press).
HASSIN, R. AND HAVIV, M. (2003), *To Queue or Not to Queue: Equilibrium Behavior in Queueing Systems*, Vol. 59 (New York, NY: Springer Science & Business Media).
HAYASHI, F. AND MANIFF, J. L. (2019), "Public Authority Involvement in Payment Card Markets: Various Countries—August 2019 Update" (Federal Reserve Bank of Kansas City).

HERKENHOFF, K. F. AND RAVEENDRANATHAN, G. (2020), "Who Bears the Welfare Costs of Monopoly? The Case of the Credit Card Industry" (Technical Report, National Bureau of Economic Research).
HUBERMAN, G., LESHNO, J. D. AND MOALLEMI, C. (2019), "An Economist's Perspective on the Bitcoin Payment System", in *AEA Papers and Proceedings*, Vol. 109. 93–96.
KITTSTEINER, T. AND MOLDOVANU, B. (2005), 'Priority Auctions and Queue Disciplines that Depend on Processing Time', *Management Science,* **51**, 236–248.
KLEINROCK, L. (1975), *Queueing Systems. Volume 1: Theory* (Wiley-Interscience).
KROLL, J. A., DAVEY, I. C. AND FELTEN, E. W. (2013), "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries", in *The Twelfth Workshop on the Economics of Information Security (WEIS 2013)*.
LAVI, R., SATTATH, O. AND ZOHAR, A. (2017), "Redesigning Bitcoin's Fee Market" arXiv preprint arXiv:1709.08881.
LESHNO, J. D. AND STRACK, P. (2020), "Bitcoin: An axiomatic approach and an impossibility theorem" *American Economic Review: Insights*, **2**, 269–286.
LUI, F. T. (1985), "An Equilibrium Queuing Model of Bribery", *Journal of Political Economy,* **93**, 760–781.
MAKAROV, I. AND SCHOAR, A. (2018), "Trading and Arbitrage in Cryptocurrency Markets" (Working Paper).
MCKINSEY and COMPANY (2019), "Global Payments Report 2019: Amid Sustained Growth, Accelerating Challenges Demand Bold Actions" https://www.mckinsey.com/ /media/mckinsey/industries/financial services/our insights/tracking the sources of robust payments growth mckinsey global payments map/global-payments-report-2019-amid-sustained-growth-vf.ashx.
MORNINGSTAR (2019), "Visa Inc Class a Analysis" (Economic Moat by Brett Horn, Updated 17 December 2019).
NAKAMOTO, S. (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System" (White Paper).
NARAYANAN, A., BONNEAU, J., FELTEN, E., et al. (2016), *Bitcoin and Cryptocurrency Technologies* (Princeton, NJ: Princeton University Press).
OLVER, F. J. W., LOZIER, D. W., BOISVERT, R. F. et al., eds (2010), *NIST Handbook of Mathematical Functions* (Cambridge, MA: Cambridge University Press).
PAGNOTTA, E. AND BURASCHI, A. (2018), "An Equilibrium Valuation of Bitcoin and Decentralized Network Assets" (Working Paper).
PASS, R., SEEMAN, L. AND SHELAT, A. (2017), "Analysis of the Blockchain Protocol in Asynchronous Networks", in Coron, JS., Nielsen, J. (eds) *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Vol. 10211 (Cham: Springer) 643–673.
PRAT, J. AND WALTER, B. (2018), "An Equilibrium Model of the Market for Bitcoin Mining" (CESifo Working Paper Series No. 6865).
RON, D. AND SHAMIR, A. (2013), "Quantitative Analysis of the Full Bitcoin Transaction Graph", in *International Conference on Financial Cryptography and Data Security* (Springer) 6–24.
ROSENBAUM, A., BAUGHMAN, G., MANUSZAK, M. D., STEWART, K., HAYASHI, F. and STAVINS, J. (2017), "Faster Payments: Market Structure and Policy Considerations" (Federal Reserve Bank of Kansas City Working Paper No. RWP) 17–14.
SAPIRSHTEIN, A., SOMPOLINSKY, Y. AND ZOHAR, A. (2016), "Optimal Selfish Mining Strategies in Bitcoin", in *International Conference on Financial Cryptography and Data Security* (Berlin, Heidelberg: Springer) 515–532.
SCHILLING, L. AND UHLIG, H. (2018), "Some Simple Bitcoin Economics" (NBER Working Paper No. 24438).
SOCKIN, M. AND XIONG, W. (2018), "A Model of Cryptocurrencies" (Working Paper).
SOMPOLINSKY, Y. AND ZOHAR, A. (2015), "Secure High-rate Transaction Processing in Bitcoin", in *International Conference on Financial Cryptography and Data Security*, (Springer) 507–527.
TANENBAUM, A. S. AND VAN STEEN, M. (2007), *Distributed Systems: Principles and Paradigms* (Upper Saddle River, NJ: Prentice-Hall).
UNITED STATES CONG. HOUSE COMMITTEE ON FINANCIAL SERVICES TASK FORCE ON FINANCIAL TECHNOLOGY (2020), "Is Cash Still King? Reviewing the Rise of Mobile Payments", *116th Cong. 2nd Sessions Testimony of Aaron Klein, Fellow, Economic Studies* (Brookings Institution).
WRIGHT, J. (2012), "Why Payment Card Fees are Biased Against Retailers", *The RAND Journal of Economics,* **43**, 761–780.
YAO, A. C.-C. (2018), "An Incentive Analysis of Some Bitcoin Fee Design" arXiv preprint arXiv:1811.02351.
YERMACK, D. (2015), "Is Bitcoin a Real Currency? An Eonomic Appraisal", in Lee Kuo Chuen, D. (ed) *Handbook of Digital Currency* (Elsevier, Academic Press) 31–43.
ZOHAR, A. (2015), "Bitcoin: Under the Hood", *Communications of the ACM,* **58**, 104–113.