Journal of Financial Economics 144 (2022) 347–369

Contents lists available at ScienceDirect

Journal of Financial Economics

journal homepage: www.elsevier.com/locate/jfec

Bitcoin's limited adoption problem

Franz J. Hinzen[a], Kose John[a], Fahad Saleh[b,*]

[a] *New York University Stern School of Business, 44 West 4th Street, New York, NY 10012, USA*
[b] *Wake Forest University, 1834 Wake Forest Rd, Winston-Salem, NC 27109, USA*

ARTICLE INFO

Article history:
Received 16 December 2021
Revised 26 January 2022
Accepted 26 January 2022

JEL classification:
E42
G00
G29

Keywords:
Bitcoin
Limited adoption
Consensus
Network delay
Blockchain
Fintech

ABSTRACT

We demonstrate theoretically that Bitcoin's limited adoption arises as an equilibrium outcome rather than as a short-lived property. Our results are driven by negative network effects which arise due to Bitcoin's need for consensus and the existence of network delay. As the Bitcoin network expands, network delay grows thereby prolonging the time needed for generating consensus. In turn, transaction settlement becomes prolonged, and users abandon the system, yielding limited adoption. Increasing transaction rates fails to solve this problem because increasing transaction rates increases fork probabilities which prolongs the consensus process and generates limited adoption.

1. Introduction

Bitcoin was proposed by Nakamoto (2008) with the goal of becoming a widely adopted decentralized payment system. To date, however, Bitcoin remains sparsely adopted as a payment system. Accordingly, a natural question becomes whether Bitcoin's economic design is compatible with its goal. This paper answers that question by demonstrating that Bitcoin's design makes limited adoption an equilibrium outcome.

Our results arise because we uncover the existence of negative network effects within Bitcoin's design. These negative network effects distinguish Bitcoin from traditional centralized payment systems and serve as the driving force for its limited adoption. To understand how negative network effects arise, we emphasize that a blockchain constitutes a unique electronic ledger that is stored among a potentially large network of agents commonly referred to as *miners*. Bitcoin's design implies that miners are likely to possess inconsistent ledgers at certain times, but such inconsistencies must be reconciled for Bitcoin to be viable because a transaction is deemed settled only if all miners agree on it being on the ledger. Our analysis uncovers that achieving agreement among miners, commonly referred to as *consensus*, becomes more difficult as the mining network size increases which, in turn, contributes to negative network effects.

The economics literature has thus far overlooked the negative network effects from Bitcoin. That oversight arises because theoretical analyses of Bitcoin typically neglect to model *network delay* which refers to the time required to communicate information across the mining network. A novel feature of our analysis is that we incorporate network delay which, together with the need for consensus, generates negative network effects. To understand this point, we highlight that miners cannot agree on any par-

[*] Corresponding author.
E-mail addresses: fhinzen@stern.nyu.edu (F.J. Hinzen), kjohn@stern.nyu.edu (K. John), salehf@wfu.edu (F. Saleh).

https://doi.org/10.1016/j.jfineco.2022.01.003
0304-405X/© 2022 Elsevier B.V. All rights reserved.

ticular information unless they are all aware of that information. Network delay is relevant because it corresponds to the time required for new information to become common information across the network. As we discuss in Section 2.3, network delay imposes limits upon the ability to generate consensus expeditiously even when miners attempt to coordinate. Our analysis highlights that these limits contribute to prohibitive delays for Bitcoin users and consequently induce limited adoption.

We model Bitcoin as a queuing system in which miners service a set of users. Each user has a unit transaction demand and derives utility from her transaction being settled on the blockchain. Users have a heterogeneous disutility for waiting. Each user may pay a transaction fee to reduce her expected wait time, but each user also incurs disutility in proportion to the fee paid. Therefore, each user selects a fee level in equilibrium to optimally balance her dislike for waiting with that of paying a fee. If her optimal utility from using Bitcoin falls below a reservation level then she chooses to abandon Bitcoin, and we classify this choice as non-adoption. The reservation level reflects the existence of an outside option so that not adopting Bitcoin implies transacting via a traditional alternative payment system.

Our first main result, Proposition 2, highlights that Bitcoin cannot maintain a non-negligible adoption rate when transaction demand becomes large. We deem this inability to maintain a non-negligible adoption rate for large transaction demands as *limited adoption*, which aligns our meaning of limited adoption with common usage. To understand how our meaning of limited adoption aligns with common usage, we offer a simple fact: Bitcoin is used by more people than certain developed economy fiat currencies, but Bitcoin's adoption rate among all people is trivial whereas those developed economy fiat currencies possess a near-universal adoption rate within their respective countries. To give a concrete example, New Zealand has approximately 5 million people within its borders whereas over 30 million people use Bitcoin. Nonetheless, the New Zealand Dollar (NZD) is not considered sparsely adopted, and Bitcoin is not considered widely adopted as a payment system. The referenced framing arises because the adoption rate of NZD in New Zealand is approximately 100% whereas the adoption rate of Bitcoin almost anywhere in the world is less than 1%. Thus, we focus on the adoption rate rather than the raw number of users. Moreover, we examine the adoption rate as transaction demand becomes large because we seek to understand how widely adopted Bitcoin could become if it were to compete directly with traditional payment systems which experience large transaction demands.

We relate the aforementioned result to three features of Bitcoin: the need for consensus among miners, free entry with respect to the mining network, and a supply constraint on the transaction rate. As discussed, the need for consensus arises because the blockchain is a unique ledger, and disagreement implies that miners possess different ledgers. Free entry is directly imposed within Bitcoin by the fact that serving as a miner requires no special permission, implying that mining is feasible but not necessarily incentive-compatible for all agents. As previously noted, users may pay fees to reduce wait times, and those fees are paid to miners. Potential miners trade off the benefits from earning those fees against the costs of participating in the mining process. Accordingly, our analysis imposes a free-entry condition by determining the set of active miners as those for whom mining is economically profitable. The supply constraint on the transaction rate refers to an observed fact of Bitcoin. More precisely, the Bitcoin ledger updates approximately every 10 min and that rate of updating corresponds to a supply constraint on the transaction rate.

Proposition 2 arises from a straight-forward economic analysis. The supply constraint on Bitcoin's transaction rate implies that prices rather than quantities primarily respond to an increase in transaction demand. Thus, heightened transaction demand endogenously generates an increase in fees (i.e., the price for expedited service). The fee increase, in turn, augments expected revenues from serving as a miner. The mining network's free entry condition then implies that additional miners enter the network. The resulting network expansion exacerbates network delay which, due to the need for consensus, prolongs expected user wait times. The prolonged user wait times then drive users away from Bitcoin towards the traditional alternative so that a shrinking fraction of users actually adopt Bitcoin. Accordingly, Proposition 2 establishes that Bitcoin cannot maintain a non-negligible adoption rate when facing heightened demand - we term this problem the *limited adoption problem*.

A natural response to the described limited adoption problem might be to propose that Bitcoin adopt a flexible transaction rate that expands in the presence of heightened demand. While such a proposal may succeed in a traditional setting, we find that it fails in the case of Bitcoin due to Bitcoin's decentralized economic design, which requires consensus and makes network delay an important constraint. We formalize that point via our second main result, Proposition 3.

To convey the intuition from Proposition 3, we offer an example of how an expansion of processing rates solves limited adoption in a traditional setting and contrast that with Bitcoin's context. For the example of a traditional setting, we consider a grocery store. Just as Bitcoin might face a heightened demand for transactions, the grocery store might face a heightened demand for check out by customers. Nonetheless, the grocery store's heightened demand need not lead to prohibitive wait times and customers abandoning the store (akin to limited adoption) because the grocery store could counter the heightened demand by increasing the number of check-out counters (i.e., increasing the processing rate). The increased processing rate would then reduce wait times, thereby solving the problem. In contrast, the analogous action of increasing Bitcoin's transaction rate fails to solve the limited adoption problem for Bitcoin. This failure arises precisely because of the need for consensus and the relevance of network delay. Importantly, within a grocery store, the cashiers need not jointly agree upon one sequence of customers (i.e., they do not need to attain consensus); rather, the cashiers conduct parallel processing without any need to communicate thereby rendering communication time (akin to network delay) irrelevant. If the cashiers were required to communicate with each other and converge upon a single sequence of customers processed across all cashiers (akin to consensus), then increasing the number of cashiers would not solve the problem because that increase would exacerbate communication difficulties. Those communication difficulties would then generate delays, leading to prolonged customer wait times. Similarly, within Bitcoin, increasing the transaction rate increases the time needed to achieve consensus which then generates prohibitive user wait times and thus results in limited adoption.

We distinguish between the Bitcoin payment system and its native asset, bitcoin, with our focus being on the former. Importantly, our results do not preclude the success of bitcoin as an asset. Rather, we demonstrate that such success is unlikely to be driven by adoption of the underlying payment system so that bitcoin should be viewed as something other than as a medium of exchange. Recent work supports this view, demonstrating that transactional benefits can explain only a trivial fraction of bitcoin price movements (see Biais et al., 2020).

Our results apply to Bitcoin and similar blockchains but do not apply to blockchains in general. In particular, as we discuss in Section 5, there are a variety of blockchain proposals that potentially overcome limited adoption although those proposals remain understudied among economists. Some particularly compelling proposals include Bitcoin NG, modern Proof-of-Stake protocols and permissioned blockchains.

Our paper relates to a large literature that studies the economics of Bitcoin. John et al. (2022) provide a survey of that literature. Moreover, some notable works within that literature include Yermack (2015), Biais et al. (2019), Easley et al. (2019), Foley et al. (2019), Raskin et al. (2019), Biais et al. (2020), Chiu and Koeppl (2020), Griffin and Shams (2020), Makarov and Schoar (2020), Alsabah and Capponi (2021), Cong et al. (2021a), Huberman et al. (2021) and Pagnotta (2022). Papers closely related to our work include Cong et al. (2021b) and Iyengar et al. (2022). In particular, both Cong et al. (2021b) and Iyengar et al. (2022) also study blockchain adoption, but neither examine the specific context of Bitcoin. Iyengar et al. (2022) study blockchain adoption in a business context, whereas Cong et al. (2021b) abstract from network delay, which is a key friction for Bitcoin as our results establish.

Our work also relates to a part of the computer science literature that offers solutions for scaling blockchains. That literature provides technical specifications but not economic analyses. More concretely, the referenced literature does not model user preferences nor endogenous adoption decisions so that our work serves as an economic complement to it. For a survey of prominent ideas from the referenced literature, the interested reader may consult Zhou et al. (2020).

2. Model

We model an infinite horizon setting with two types of agents, users and miners. Our setting also involves two types of payment systems, Bitcoin and a traditional alternative. We assume that each user possesses unit transaction demand and conducts that transaction via either Bitcoin or the traditional alternative. Transactions are added to the Bitcoin blockchain by miners who receive fees, endogenously selected by users, for processing those transactions. The remainder of this section presents our model in detail.

2.1. Users

At $t = 0$, $N \geq 2$ users arrive simultaneously. Each user possesses unit transaction demand and satisfies that demand using either Bitcoin or a traditional alternative.

User $i \in \{1, \ldots, N\}$ possesses type $c_i \sim U[\underline{c}, \overline{c}]$ which corresponds to her disutility towards waiting for her transaction to be processed. We assume that $\overline{c} > \underline{c}$ so that there exists heterogeneity among users (i.e., $\mathbb{P}(c_i = c_j) = 0$ for $i \neq j$). We also assume that $\underline{c} > 0$ so that all users are impatient (i.e., $c_i > 0$ for all i). We let $W(f, f_{-i})$ denote User i's wait time when she pays fee $f \geq 0$ with f_{-i} denoting the equilibrium fees paid by other users. In turn, User i's total expected disutility from waiting equals $c_i \cdot \mathbb{E}[W(f, f_{-i})]$ when she pays fee f. We further assume that User i earns endogenous utility $R_1 \cdot (\pi_* N)^\alpha + R_0$ from transacting via Bitcoin where $R_0, R_1 \in \mathbb{R}_+$ and $\alpha \in (0, 1)$ are exogenous parameters, whereas $\pi_* \in [0, 1]$ denotes the endogenous *adoption rate* of Bitcoin.[1] In turn, $\pi_* N$ represents the endogenous *adoption level* of Bitcoin. User i's total utility from transacting via Bitcoin equals $R_1 \cdot (\pi_* N)^\alpha + R_0 - c_i \cdot \mathbb{E}[W(f, f_{-i})] - f$ when she pays fee f. We model the traditional alternative as an outside option with utility from using it normalized to 0. Therefore, User i solves:

$$\max\{ \max_{f \geq 0} R_1 \cdot (\pi_* N)^\alpha + R_0 - c_i \cdot \mathbb{E}[W(f, f_{-i})] - f, \ 0\} \tag{1}$$

We assume that user types are private information but the distribution from which types are drawn is common knowledge (i.e., User i does not know c_j for $j \neq i$ but knows $c_j \sim U[\underline{c}, \overline{c}]$). Accordingly, the expectation over wait times is taken over the equilibrium fees of other users, each of which will depend upon the type of the respective user. Miners optimally process transactions in descending fee order so that a higher fee improves the probability that a user receives service sooner. Each user trades off the disutility from paying a higher fee with the utility gain from a reduction in her expected wait time and thereby selects an optimal fee in equilibrium. If $R_1 \cdot (\pi_* N)^\alpha + R_0 - c_i \cdot \mathbb{E}[W(f_i, f_{-i})] - f_i \geq 0$, with $f_i \geq 0$ denoting User i's optimal fee, then User i transacts via Bitcoin. Otherwise, User i employs the traditional alternative. This adoption choice follows from the user's access to a traditional alternative that confers her a utility of 0.

Akin to Huberman et al. (2021), we examine cut-off equilibria with the cut-off denoted by $c_* \in [\underline{c}, \overline{c}]$. More precisely, we solve for equilibria such that the set of users that adopt is given by $\{i : c_i \leq c_*\}$ with User c_* being referred

[1] We impose $R_0 > \underline{R}$ to rule out a trivial equilibrium in which no user adopts Bitcoin, which we define formally later in this section. Explicitly, $\underline{R} = \underline{c} \cdot (\frac{1}{\Lambda} + \tau(\Lambda, \Delta(\frac{B}{\beta}))$ where B, β, Λ, $\Delta(\cdot)$ and $\tau(\cdot, \cdot)$ are introduced later in this section.

to as the marginal user hereafter. We define the adoption rate, π_*, as the expected proportion of users that adopt Bitcoin (i.e., $\pi_* \equiv \mathbb{P}(c_i \leq c_*)$). Consequently, the cut-off, c_*, possesses a bijective relationship with the adoption rate, π_*, as follows:

$$\pi_* = \frac{c_* - \underline{c}}{\bar{c} - \underline{c}}, \qquad c_* = (\bar{c} - \underline{c}) \cdot \pi_* + \underline{c} \tag{2}$$

2.2. Miners

A miner refers to a member of the Bitcoin network that stores a copy of the Bitcoin ledger and "mines" to update the ledger. As a convention, we use "miner" to refer to a single computer processor that participates in the Bitcoin network. This convention does not preclude that multiple processors might be controlled by the same agent. In fact, we discuss the implications of such centralization in Section 5.1 although our main results hold for arbitrary mining market structures.

Each miner must pay some cost $\beta > 0$ to acquire mining technology. We assume that each processor possesses identical hashing power so that each miner expects to earn an equal share of fees among all miners.[2] Our analysis focuses on transaction fees, but we allow that there exists a block reward, B, paid to miners.[3] Then, assuming risk neutral preferences, each miner solves:

$$\max\{\ \frac{1}{M}\Big(B + \mathbb{E}[\sum_i f_i]\Big) - \beta,\ 0\} \tag{3}$$

M denotes the equilibrium number of miners so that the pay-off from mining equals $\frac{1}{M}\Big(B + \mathbb{E}[\sum_i f_i]\Big)$ whereas the pay-off from not mining equals 0. Bitcoin's design allows for free entry among miners, so miners must be indifferent between mining and not mining. Accordingly, we impose the following free entry condition in equilibrium:

$$M = \frac{B + \mathbb{E}[\sum_i f_i]}{\beta} \tag{4}$$

As an aside, our model assumes that miners are patient. Accordingly, miners do not discount their fee revenues and the total expected present value of mining revenues equals $B + \mathbb{E}[\sum_i f_i]$ directly.[4] Our assumption regarding miners being perfectly patient is a simplification to reflect that miners are significantly more patient than users seeking casual transactions. More precisely, an hour long wait for a casual transaction would likely dissuade a user from using Bitcoin for a purchase. In contrast, mining is a business and earning revenues an hour (or even days) later would be practically immaterial.

2.3. Blockchain

A blockchain constitutes an electronic ledger. Users submit transactions which are accumulated by miners in discrete chunks called *blocks*. In turn, the blocks are placed in a *chain* with a specific order, hence the term blockchain.

Blocks have a fixed maximal size, and a block can be added to the existing chain of blocks only if the block is *valid*. Within the setting of Bitcoin, a block is valid if it solves a trivial but computationally intensive puzzle.[5] The block generation process is of economic importance because it regulates the rate at which transactions enter the blockchain which, in turn, affects user utility through user wait times.

The process by which a single miner produces a valid block is well-known to be approximated by a Poisson process so that prior literature generally assumes that each miner generates valid blocks exactly according to a Poisson process.[6] We also adopt that assumption, but we depart from prior literature with regard to our modeling of blocks that ultimately enter the blockchain. In particular, our analysis incorporates the fact that all valid blocks do not necessarily enter the blockchain. This fact holds true because valid blocks might not be consistent with each other and thus some valid blocks might have to be discarded. The possibility for valid blocks to be inconsistent with each other is well known and is referred to as a *fork*.[7]

We first qualitatively explain the source of forks within our analysis and then state our formal model of the blockchain. Our analysis assumes that miners attempt to co-ordinate. More precisely, each Miner $j \neq i$ accepts a valid block sent by Miner i if Miner i's block is consistent with the blockchain already stored by Miner j when

[2] This assumption is appropriate since most miners use the same type of specialized computing hardware (see Alsabah and Capponi, 2021 and Ferreira et al., 2020).

[3] We assume that $B > \beta$ which ensures that it is incentive compatible for at least one processor to participate in mining.

[4] It is important to recognize that while our model considers consensus delays, our model never generates perpetual disagreement. Rather, within our model, consensus always obtains eventually with probability one. As a consequence, miners being patient implies that the expected present value of mining revenues equals the expected sum of block rewards and fees: $B + \mathbb{E}[\sum_i f_i]$.

[5] See de Vries (2018), Chiu and Koeppl (2020) and Saleh (2019) for details regarding the magnitude of energy expenditure and associated welfare implications.

[6] Formally, the number of valid blocks produced by a miner in any interval of T time units is given exactly by $\#(T) := \sum_{n=1}^{N_B \cdot T} X_n$ where N_B denotes the number of attempts per unit time and X_n denotes an indicator equaling one if and only if the nth attempt was successful. The Bitcoin computational puzzle is specified such that $\{X_n\}_{n=1}^{\infty}$ is an independent and identically distributed sequence. Then, letting $\rho := \mathbb{P}(X_n = 1)$ denote the probability that an individual attempt succeeds, the Poisson Limit Theorem (PLT) implies that $\#(T) \xrightarrow{d} Poisson(\lambda \cdot T)$ as $N_B \to \infty$ when $\rho \to 0^+$ with $\lambda := \lim_{N_B \to \infty} \rho \cdot N_B$. Thus, if the number of attempts per unit time is large (i.e., N_B is large) and the likelihood that each attempt succeeds is small (i.e, ρ is near zero), then PLT establishes that the number of blocks produced by a given miner, $\#(T)$, is approximated by a Poisson process. In practice, both aforementioned hypotheses are met because attempts are conducted by specialized computing units so that N_B is large, and the computational puzzle is difficult so that ρ is close to zero.

[7] A fork may arise due to network delay or due to misaligned miner incentives. Biais et al. (2019) study forks which arise due to misaligned miner incentives whereas we focus upon forks that arise due to network delay. Decker and Wattenhofer (2013) indicate that Bitcoin forks arise largely due to network delay, and our analysis (see Proposition 3) indicates that such forks become especially problematic when the transaction rate of the blockchain is increased.

Miner j first receives news of Miner i's block. If any Miner $j \neq i$ finds that Miner i's block is not consistent with her blockchain when she first receives news of Miner i's block then she rejects the block and a fork arises due to a disagreement between Miners i and j. Under such an assumption, if all miners initially store the same blockchain (i.e., the blockchain is in a state of consensus) then Miner i's block will not correspond to a fork if no Miner $j \neq i$ produces a valid block before receiving news of Miner i's block. This fact holds because two blocks are necessarily inconsistent with each other if they are produced without knowledge of each other.[8] Intuitively, if Miner $j \neq i$ produces a valid block after Miner i but before receiving news of Miner i's block then Miner i and j disagree on the temporal order of their two blocks because each miner believes that her block was produced first. As the two blocks are inconsistent with each other, each miner must select only one of the two blocks. Since either a time-ordering rule or even personal self-interest would lead to each miner selecting her own block, a fork results (i.e., lack of consensus obtains).

To incorporate forks into our model, we proceed by determining the probability that a given valid block corresponds to a fork:

$$\mathbb{P}(Fork) = 1 - e^{-\Lambda \Delta(M)} \tag{5}$$

Λ denotes the transaction rate, and $\Delta(M)$ denotes the network delay for a normalized single-transaction block averaged over all pairs of the M miners in the network. Equation (5) highlights that the fork probability increases in both the transaction rate and the network delay for normalized block; we establish that relationship in Appendix A and defer associated technical details to that section. Among other results, Appendix A demonstrates an equivalence between modifying block sizes and modifying block rates so that changes in the transaction rate, Λ, may be analyzed without specific attention to whether such changes are implemented by modifying the block size or the block rate. Accordingly, we normalize the block size to a single transaction hereafter.

We assume that miners must agree on $b \in \mathbb{N}_+$ consecutive blocks to regain consensus regarding the entire blockchain's contents when the blockchain is not already in a state of consensus. All our results hold even for $b = 1$ which corresponds to assuming that consensus on the entire blockchain's content requires only agreement on the most recent block. In general, agreement on a single block need not imply consensus on the full chain. Thus, our findings highlight that limited adoption arises for Bitcoin even with generous assumptions regarding generating consensus.

To complete our model specification, we now clarify our assumptions regarding $\Delta(M)$, the network delay. We model $\Delta(M)$ in general terms as any function that satisfies the following two conditions: $\Delta(1) = 0$, and $\Delta'(M) > 0$ for $M > 1$. The first condition, $\Delta(1) = 0$, asserts only that a network with one miner (i.e., a centralized network) possesses no network delay. The second condition states that network delay increases as the network size increases beyond a single miner. The first condition is self-evident (i.e., communication with oneself requires no time) whereas the second assumption is consistent with the random network topology of Bitcoin (see Chung and Lu, 2002 and Riordan and Wormald, 2010).

2.4. Equilibrium

We formally define an equilibrium as follows:

Definition 1. Bitcoin Equilibrium

Our Bitcoin model is parameterized by the number of users, N, three parameters relating to the blockchain utility for each user, R_0, R_1 and α, and the blockchain transaction rate, Λ. The N users possess types, $\{c_i\}_{i=1}^N$, with $c_i \sim U[\underline{c}, \overline{c}]$. A Bitcoin Equilibrium is (1) an adoption cut-off, c_*, (2) a function, $\phi(c)$, that maps user types to their fees, (3) a set of fee realizations for the N users, $\{f_i\}_{i=1}^N$, and (4) a mining network size, M. The equilibrium satisfies the following conditions:

(i) A User Adopts Bitcoin Iff Doing So Is Optimal A user adopts Bitcoin (i.e., $c_i \le c_*$) if and only if doing so is optimal.
(i.e., for all $c \le c_* \Leftrightarrow \max\limits_{f \ge 0} \; R_1 \cdot (\pi_* N)^\alpha + R_0 - c \cdot \mathbb{E}[W(f, f_{-i})] - f \ge 0$ where $\pi_* = \frac{c_* - \underline{c}}{\overline{c} - \underline{c}}$)

(ii) Equilibrium User Fees Depend Upon User Types
User i pays a fee, f_i, which depends on her type, c_i. (i.e., for all $i : f_i = \phi(c_i)$)

(iii) Equilibrium Fee Function Provides Optimal Bitcoin Fees
The fee function, $\phi(c_i)$, provides optimal Bitcoin fees. In particular, the user maximizes her utility from using Bitcoin if she adopts Bitcoin (i.e., $\phi(c)$ solves $\max\limits_{f \ge 0} \; R_1 \cdot (\pi_* N)^\alpha + R_0 - c \cdot \mathbb{E}[W(f, f_{-i})] - f$ if $c \le c_*$) but pays zero fees to Bitcoin otherwise (i.e., $\phi(c) = 0$ if $c > c_*$) because, per Condition i, using Bitcoin is not optimal in that case (i.e., $\max\limits_{f \ge 0} \; R_1 \cdot (\pi_* N)^\alpha + R_0 - c \cdot \mathbb{E}[W(f, f_{-i})] - f < 0$ if $c > c_*$).

(iv) A User Receives Settlement After Higher Priority Users And When Consensus Next Obtains
User i's wait time, $W(f, f_{-i})$, if she pays fee f depends not only on f but also on other user fees, f_{-i}. More precisely, transactions are processed in descending fee order so that User i must wait $\sum_{j: f \le f_j} H_j$ with H_j denoting the service time for User j and $\{j : f \le f_j\}$ denoting the set of users paying higher fees.[9] Further, User i's transaction is not settled even after her transaction enters the blockchain unless the blockchain is at consensus. We denote the (random and possibly zero) time until consensus next obtains by Z_i.[10] Thus, our user wait function becomes:

$$W(f, f_{-i}) = \sum_{j: f \le f_j} H_j + Z_i$$

[8] Knowledge of each other is necessary because the puzzle being solved depends upon the entire chain of blocks to which the new block is being appended. For further details, the interested reader may consult John et al. (2022).

[9] Recall that we normalize the block size to one transaction per block.

[10] We detail the properties of Z_i in Appendix B.

(v) The Mining Market Is Characterized By Free Entry
The total expected cost of mining, β, equals the total expected profit from mining, $\frac{1}{M}\left(B+\mathbb{E}[\sum_i f_i]\right)$, for each miner. (i.e, $\beta=\frac{1}{M}\left(B+\mathbb{E}[\sum_i f_i]\right)$)

Definition 1 simply summarizes the discussion from Sections 2.1–2.3, condensing it into an equilibrium definition. Therefore, we do not elaborate further on our equilibrium definition except that we note now that we assume the blockchain's stationary distribution characterizes its initial state.[11] The subsequent result establishes equilibrium existence:

Proposition 1. Bitcoin Equilibrium

There exists a Bitcoin Equilibrium. The following conditions characterize that equilibrium with $\tau(\Lambda,\Delta(M))\equiv\mathbb{E}[Z_1]$, $\Psi(\Lambda,\Delta(M))\equiv\frac{1}{\Lambda}+\tau(\Lambda,\Delta(M))$ *and* $M(c)\equiv\frac{B}{\beta}+\frac{N(N-1)}{6\beta\Lambda}\frac{(c-\underline{c})\cdot(c^2+c\cdot\underline{c}-2\underline{c}^2)}{(\bar{c}-\underline{c})^2}$:

(A) $\phi(c)=\frac{N-1}{\bar{c}-\underline{c}}\times\frac{c^2-\underline{c}^2}{2\Lambda}$ *if* $c\le c_*$ *and* $\phi(c)=0$ *otherwise.*
(B) $M=M(c_*)$.
(C) *If* $R_1\cdot N^\alpha+R_0<\bar{c}\cdot\Psi(\Lambda,\Delta(M(\bar{c})))+(N-1)\times\frac{\bar{c}+\underline{c}}{2\Lambda}$, *then* $c_*\in(\underline{c},\bar{c})$ *and* c_* *solves:*
$R_1\cdot(\frac{c_*-\underline{c}}{\bar{c}-\underline{c}})^\alpha\cdot N^\alpha+R_0=c_*\Psi(\Lambda,\Delta(M(c_*)))+\frac{N-1}{\bar{c}-\underline{c}}\times\frac{c_*^2-\underline{c}^2}{2\Lambda}$
(D) *If* $R_1\cdot N^\alpha+R_0\ge\bar{c}\cdot\Psi(\Lambda,\Delta(M(\bar{c})))+(N-1)\times\frac{\bar{c}+\underline{c}}{2\Lambda}$, *then a full adoption equilibrium arises:*
$c_*=\bar{c}\Longleftrightarrow\pi_*=1$

We follow prior literature and require that ϕ *constitutes a strictly increasing and twice differentiable function on the interval* $(\underline{c},c_*)$. *In such a case, any equilibrium must satisfy the above conditions, and we prove that at least one such equilibrium exists for any set of parameters.*

Proposition 1 (A) characterizes the equilibrium fee function. This fee function is such that each user's optimal fee equals the function evaluated at the user's type (i.e., $f_i=\phi(c_i)$) when each user anticipates that all other users select fees according to the same fee function (i.e., for all $j\neq i: f_j=\phi(c_j)$). More formally, as required by Definitions 1 (ii) and (iii), ϕ is a function that solves the following problem:

$$\phi(c_i)=\underset{f\ge0}{\arg\max}\ R_1\cdot(\pi_*N)^\alpha+R_0-c_i\cdot\mathbb{E}[W(f,\phi(c_{-i}))]-f \tag{6}$$

for all c_i with $\phi(c_{-i})\equiv\underset{j:j\neq i}{\times}\phi(c_j)$ so that $\phi(c_{-i})$ corresponds to the equilibrium fees of all users other than User i.

Note that the equilibrium fee function implies that any user who prefers to use the traditional alternative instead of the blockchain pays no fees (i.e., $\phi(c_i)=0$ for all $c_i>c_*$). That behavior is optimal because user utility decreases in the level of the fee so that a zero fee is trivially optimal when a user does not use Bitcoin. In contrast, users who transact via the blockchain in equilibrium (i.e., any User i such that $c_i\le c_*$) pay fees according to:

$$\phi(c_i)=\frac{N-1}{\bar{c}-\underline{c}}\times\frac{c_i^2-\underline{c}^2}{2\Lambda} \tag{7}$$

which highlights that a user's equilibrium fee increases in transaction demand and the user's wait disutility (i.e., $\phi(c_i)$ increases in N and c_i) but decreases in the blockchain's transaction rate (i.e., $\phi(c_i)$ decreases in Λ). Fees increasing in transaction demand and decreasing in the blockchain's transaction rate both reflect that fees increase in congestion. Fees increasing in a user's wait disutility reflects that a high-wait-disutility user values a reduction in wait time more so than a low-wait-disutility user, leading the former to pay a higher fee in equilibrium.

Proposition 1 (B) characterizes the equilibrium number of miners, $M(c_*)$, in an equilibrium where c_* denotes the adoption cut-off. This condition arises directly from applying the equilibrium fee function to the free entry condition of the mining market, given by Definition 1 v.

Proposition 1 (C) characterizes the adoption cut-off in the case that there exists a user indifferent between using the blockchain and using the traditional alternative. In such a case, the cut-off user (i.e., any User i such that $c_i=c_*$) gains no utility from transacting via the blockchain since, as discussed, we normalize the utility of the traditional alternative to zero. In turn, this implies that the utility from transacting via the blockchain, $R_1\cdot(\pi_*N)^\alpha+R_0=R_1\cdot(\frac{c_*-\underline{c}}{\bar{c}-\underline{c}})^\alpha\cdot N^\alpha+R_0$, must equal the sum of the wait disutility, $c_*\Psi(\Lambda,\Delta(M(c_*)))$, and the fees paid, $\phi(c_*)=\frac{N-1}{\bar{c}-\underline{c}}\times\frac{c_*^2-\underline{c}^2}{2\Lambda}$.

Proposition 1 (D) characterizes the adoption cut-off in the case that all users weakly prefer transacting via the blockchain. In this case, $c_*=\bar{c}\Leftrightarrow\pi_*=1$ because then any User c_i is below the adoption cut-off (i.e., $c_i\le c_*=\bar{c}$ for all i). Note that this case arises only when the exogenous utility from transacting via the blockchain with full adoption, $R_1\cdot(\pi_*N)^\alpha+R_0=R_1\cdot N^\alpha+R_0$, is sufficiently high such that even the highest-wait-disutility user (i.e., any User c_i such that $c_i=\bar{c}$) weakly prefers to use the blockchain instead of the traditional alternative (i.e., $R_1\cdot N^\alpha+R_0\ge\bar{c}\cdot\Psi(\Lambda,\Delta(M(\bar{c})))+(N-1)\times\frac{\bar{c}+\underline{c}}{2\Lambda}$).

3. Main results

We begin by considering Bitcoin with a fixed transaction rate (i.e., fixed Λ), which is consistent with Bitcoin's existing design. In that context, we demonstrate that Bitcoin faces limited adoption (Proposition 2). We then allow for a variable transaction rate within Bitcoin (i.e., we let Λ vary), and we demonstrate that our conclusion regarding Bitcoin facing limited adoption holds in that case also (Proposition 3).

Proposition 2. Limited Adoption I

Bitcoin faces limited adoption (i.e., $\lim_{N\to\infty}\pi_*=0$).

Proposition 2 provides our first main result. This result establishes that Bitcoin's adoption rate tends to zero (i.e., $\pi_*\to0$) as transaction demand diverges (i.e., $N\to$

[11] The interested reader may consult Appendix B for the explicit stationary distribution and associated technical details.

∞). Note that this result implies that Bitcoin's adoption rate is arbitrarily small for sufficiently large transaction demand. As such, Proposition 2 thus highlights that Bitcoin cannot maintain a non-trivial adoption rate if a large number of users consider Bitcoin as a feasible option.

We note that our formal characterization of limited adoption is $\lim_{N\to\infty} \pi_* = 0$. Our characterization examines $N \to \infty$ because our analysis aims to consider the Bitcoin adoption rate across the globe, and, for tractability reasons, it is easier to analyze $N \to \infty$ rather than N being some particular large number such as global transaction demand. We emphasize that $\lim_{N\to\infty} \pi_* = 0$ implies that for large N, the Bitcoin adoption rate, π_*, is close to zero hence our usage of $\lim_{N\to\infty} \pi_* = 0$ as the formal characterization of limited adoption. As a practical matter, our findings establish that Bitcoin is unlikely to become widely adopted as a payment system across the world, as initially hoped.

To provide further context, we explain the channel for Proposition 2 based on our equilibrium solutions given by Proposition 1. Per Proposition 1 (A), an increase in transaction demand exacerbates congestion, thereby raising equilibrium fees (i.e., $\phi(c)$ increases in N). Then, per Proposition 1 (B), that increase in fees generates an increase in the number of miners (i.e., M increases in N). The relationship between fees and the number of miners arises because fees correspond to revenue for miners, and the mining network is characterized by free entry so that increased fees induce entry of miners. Finally, per Proposition 1 (C), Bitcoin's adoption rate declines as the equilibrium number of miners increases (i.e., π_* decreases in M). This decrease in the adoption rate arises because the increase in the mining network size implies a commensurate increase in network delay which, in turn, prolongs user wait times (i.e., $\Psi(\Lambda, \Delta(M))$ increases in M per Lemma 10). Those increased wait times then reduce the adoption rate. Proposition 2 establishes that the adoption rate becomes arbitrarily small (i.e., $\pi_* \to 0$) as transaction demand becomes arbitrarily large (i.e., $N \to \infty$), thereby establishing limited adoption.

A natural response to the limited adoption thus far described might be to suggest Bitcoin adopt a flexible transaction rate that increases with transaction demand (i.e., Bitcoin should vary Λ with N). In fact, that proposed solution is employed in traditional settings to resolve a similar problem. For instance, in the introduction, we discuss the example of a grocery store that could experience heightened demand but overcomes the problem by increasing its processing rate. In particular, when there exists an increase in customers checking out of the grocery store (i.e., heightened demand), the store responds by increasing the number of cashiers (i.e., increasing the processing rate). In the grocery store setting, the described response keeps wait times low and thereby avoids customers abandoning the store. With that example as motivation, we subsequently explore the implications of Bitcoin allowing increased transaction rates. In contrast to the grocery store setting, we find that this policy fails to resolve the problem within the Bitcoin setting. Proposition 3 formalizes this point:

Proposition 3. Limited Adoption II

Suppose that Bitcoin's transaction rate, Λ_N, varies with transaction demand, N. Then, even in such a case, Bitcoin faces limited adoption (i.e., $\lim_{N\to\infty} \pi_* = 0$).

Proposition 3 allows that Bitcoin's transaction rate, Λ, depends upon transaction demand, N, and we hereafter acknowledge that dependence by denoting the transaction rate as Λ_N. Even allowing for such dependence, Proposition 3 establishes that Bitcoin faces limited adoption.

To understand Proposition 3, we highlight that our model implies the following decomposition for User i's expected equilibrium wait time, $\mathbb{E}_i[W(f_i, f_{-i})]$, with $\mathbb{E}_i[\cdot]$ denoting an expectation with respect to User i's information set:

$$\mathbb{E}_i[W(f_i, f_{-i})] = \underbrace{\frac{(N-1)(c_* - c_i) + 1}{\Lambda_N}}_{Traditional\ Wait\ Time} + \underbrace{\tau(\Lambda_N, \Delta(M))}_{Consensus\ Wait\ Time} \tag{8}$$

Equation (8) states that the expected wait time of each user decomposes into two terms: the traditional wait time and the consensus wait time. We refer to the first term as the traditional wait time because this component would appear even for a traditional centralized payment system. In contrast, the second term, which we refer to as consensus wait time, would not appear for a centralized payment system and therefore distinguishes Bitcoin from a centralized payment system.

The traditional wait time refers to the sum of the expected wait time for all users served before User i and the expected service time for User i. Importantly, the traditional wait time decreases in the transaction rate and vanishes as the transaction rate diverges so that it can be kept arbitrarily small by adjusting the transaction rate. To intuit this point, we note that the maximal traditional wait equals $\frac{N}{\Lambda_N}$ because even the adopting user who pays the lowest fee waits for no more than $N-1$ other users. As an example, if $N = 10$ and $\Lambda_N = 10$ transactions per second, then all users complete their traditional wait time within 1 s. If there is an increase in transaction demand with the number of potential users becoming 1000 (i.e., $N = 1000$) then increasing the transaction rate to 1000 transactions per second (i.e., $\Lambda_{1000} = 1000$) maintains the 1 s upper bound for the traditional wait time. More generally, the traditional wait time is bounded above by $\varepsilon > 0$ if $\Lambda_N = \frac{N}{\varepsilon}$. Thus, as users for a centralized payment system face only this traditional wait time, a centralized payment system may avoid limited adoption simply by increasing its transaction rate to meet demand (i.e., increasing Λ_N as N grows).

However, unlike a centralized payment system, Bitcoin cannot overcome limited adoption by increasing its transaction rate as shown by Proposition 3. That result arises because Bitcoin requires consensus among miners which, in turn, introduces an additional component to wait time that we refer to as the consensus wait time (i.e., $\tau(\Lambda_N, \Delta(M))$ appears in Eq. (8)). In fact, as we show subsequently, the consensus wait time, $\tau(\Lambda_N, \Delta(M))$, becomes prohibitive as the transaction rate increases:

Proposition 4. Consensus Wait Time Diverges with Transaction Demand

Suppose that Bitcoin adjusts its transaction rate to keep pace with transaction demand (i.e., $\lim\limits_{N\to\infty} \Lambda_N = \infty$). Then, the Consensus Wait Time, $\tau(\Lambda_N, \Delta(M))$, diverges as demand diverges, (i.e., $\lim\limits_{N\to\infty} \tau(\Lambda_N, \Delta(M)) = \infty$).

To provide some intuition regarding Proposition 4, we return to Eq. (5) which establishes that the probability a block corresponds to a fork equals $1 - e^{-\Lambda\Delta(M)}$.[12] Accordingly, a higher transaction rate, Λ, implies a higher fork probability and thus a lower probability of consensus. In turn, a lower probability of consensus on a given block implies a longer consensus wait time. In fact, Proposition 4 highlights that arbitrarily large transaction rates generate arbitrarily large consensus wait times. Thus, expected wait times diverge as transaction rates become arbitrarily large (i.e., $\lim\limits_{N\to\infty} \mathbb{E}_i[W(f_i, f_{-i})] = \infty$ when $\lim\limits_{N} \Lambda_N = \infty$ as per Eq. (8)) so that limited adoption arises even when transaction rates keep pace with transaction demand per Proposition 3.

The implication of our results as a whole is that Bitcoin faces a dilemma in the face of heightened transaction demand. Either Bitcoin keeps transaction rates fixed or it varies transaction rates with transaction demand. If Bitcoin keeps transaction rates fixed (in line with Bitcoin's current design) then Bitcoin faces prohibitive traditional wait times and, in turn, limited adoption per Proposition 2. Alternatively, if Bitcoin varies transaction rates with transaction demand then the consensus wait time becomes prohibitive thereby also generating limited adoption per Proposition 3.

We have noted that a novelty of our analysis is incorporating network delay into an economic model of blockchain. To emphasize the importance of incorporating this real-world feature that constitutes a practical constraint for Bitcoin, we provide the following result:

Proposition 5. No Adoption Problem Without Network Delay

Widespread adoption (i.e., $\lim\limits_{N\to\infty} \pi_* > 0$) can be obtained within arbitrarily large networks (i.e., $\lim\limits_{N\to\infty} M = \infty$) under the counterfactual assumption of no network delay (i.e., $\Delta(M) = 0$ for all M).

Proposition 5 establishes that Bitcoin could overcome limited adoption if it did not possess network delay. Intuitively, an absence of network delay implies that forks would never arise (i.e., $\mathbb{P}(Fork) = 0$ in Eq. (5) if $\Delta(M) = 0$). In such a case, Bitcoin would always be in a state of consensus (i.e., $\tau(\Lambda_N, \Delta(M)) = \tau(\Lambda_N, 0) = 0$) and thus could overcome limited adoption in a manner similar to a centralized payment system. Nonetheless, Bitcoin possessing no network delay is counterfactual so that Proposition 5 should be interpreted as a result that clarifies economic limitations intrinsic to Bitcoin.

4. Finite *N*

Our main findings, Propositions 2 and 3, provide limiting results (i.e., $N \to \infty$) to establish implications for adoption when demand is large (i.e., large N). In this section, we supplement those findings with results that hold for finite N. In particular, Section 4.1 demonstrates that there exists a finite adoption level for all N (i.e., $\sup\limits_{N\in\mathbb{N}} \pi_* N < \infty$). Moreover, Section 4.2 clarifies that the referenced bound falls below transaction volumes for traditional payment systems for any reasonable model parameters. The implication of our findings is thus that Bitcoin is unlikely to replace traditional centralized payment systems.

4.1. Absolute bound on adoption level

There exists a bound on Bitcoin's adoption level that applies uniformly for all N:

Proposition 6. Finite Bound on Adoption Level

There exists a finite bound on the total adoption level that applies uniformly across all levels of transaction demand. (i.e., $\sup\limits_{N\in\mathbb{N}} \pi_* N < \infty$).

Proposition 6 arises because an increase in the adoption level, $\pi_* N$, implies an increase in the endogenous fee level for the marginal user, $\phi(c_*)$. In turn, any adoption level beyond a particular finite bound cannot arise in equilibrium because any such adoption level implies a fee level that is too excessive to be consistent with such adoption levels.

More formally, Proposition 1 (C) implies the following:

$$\underbrace{R_1 \cdot \left(\frac{c_* - \underline{c}}{\bar{c} - \underline{c}}\right)^\alpha \cdot N^\alpha + R_0}_{\textit{Utility From Bitcoin}} \geq \underbrace{\frac{N-1}{\bar{c} - \underline{c}} \times \frac{c_*^2 - \underline{c}^2}{2\Lambda}}_{\textit{Marginal User Fee}} \tag{9}$$

which states that the endogenous utility from using Bitcoin must exceed the fee paid for the marginal user. Then, using Eq. (2) and applying some algebra yields:

$$R_1 + \frac{R_0}{(\pi_* N)^\alpha} \geq \frac{N-1}{N} \times \frac{c_* + \underline{c}}{2\Lambda} \times (\pi_* N)^{1-\alpha} \tag{10}$$

which reveals that arbitrarily large adoption levels cannot arise in equilibrium. In particular, letting the adoption level grow arbitrarily (i.e., $\pi_* N \to \infty$) in Eq. (10) yields $R_1 \geq \infty$, which delivers a contradiction since user utility from transacting via Bitcoin is finite (i.e., $R_0, R_1 \in \mathbb{R}_+$). Intuitively, arbitrarily large adoption levels generate arbitrarily large fees such that only an infinite utility from using Bitcoin (i.e., $R_1 = \infty$) is consistent with arbitrarily large adoption levels in equilibrium.

Proposition 6 takes the transaction rate as fixed (i.e., Λ is a fixed parameter), but that assumption is not necessary for establishing a bound on the Bitcoin adoption level. More explicitly, our next result generalizes Proposition 6 to

[12] Appendix A provides details regarding Eq. (5).

the case that the transaction rate varies with transaction demand:

Proposition 7. Finite Bound on Adoption Level II

Suppose that Bitcoin's transaction rate, Λ_N, varies with transaction demand, N. Then, even in such a case, Bitcoin faces a finite bound on its adoption level that applies uniformly across all levels of transaction demand. (i.e., $\sup_{N\in\mathbb{N}} \pi_* N < \infty$).

Proposition 7 arises for a similar reason as Proposition 3. In particular, Bitcoin faces a dilemma in the face of heightened transaction demand (i.e., when N is large). Either Bitcoin keeps transaction rates too low such that the congestion from fees ensures a finite bound on its adoption level (as per Proposition 6) or Bitcoin increases its transaction rate sufficiently fast such that wait times become prohibitive due to the need for consensus, also generating a finite bound on its adoption level. More formally, Proposition 1 (C) implies:

$$\underbrace{R_1 \cdot \left(\frac{c_* - \underline{c}}{\overline{c} - \underline{c}}\right)^{\alpha} \cdot N^{\alpha} + R_0}_{Utility\ \ From\ \ Bitcoin} \geq \underbrace{c_* \Psi(\Lambda_N, \Delta(M))}_{Marginal\ \ Wait\ \ Disutility} \tag{11}$$

which states that the endogenous utility from using Bitcoin must exceed the disutility from waiting incurred by the marginal user. Then, applying Eq. (2) and $\Psi(\Lambda_N, \Delta(M)) \equiv \frac{1}{\Lambda_N} + \tau(\Lambda_N, \Delta(M)) \geq \tau(\Lambda_N, \Delta(M))$ to Eq. (11) yields:

$$R_1 \cdot (\pi_* N)^{\alpha} + R_0 \geq c_* \tau(\Lambda_N, \Delta(M)) \tag{12}$$

and dividing through by $(\pi_* N)^{\alpha}$ implies:

$$R_1 + \frac{R_0}{(\pi_* N)^{\alpha}} \geq \frac{c_* \tau(\Lambda_N, \Delta(M))}{(\pi_* N)^{\alpha}} \tag{13}$$

In our proof for Proposition 7, we establish that the transaction rate growing sufficiently fast to avoid prohibitive fees implies that $\frac{c_* \tau(\Lambda_N, \Delta(M))}{(\pi_* \cdot N)^{\alpha}} \to \infty$ as the adoption level grows arbitrarily large (i.e., $\pi_* N \to \infty$). Consequently, if the transaction rate grows sufficiently fast to avoid prohibitive fees, Eq. (13) implies $R_1 \geq \infty$, which is a contradiction and thereby precludes arbitrarily large adoption levels. Alternatively, if the transaction rate does not grow sufficiently fast to overcome prohibitive fees, then the level of the fees themselves preclude arbitrarily large adoption levels akin to the intuition given earlier for Proposition 6.

4.2. Practical adoption limits

We provide context regarding our previous analysis with the following result:

Proposition 8. Practical Limits of Adoption

Suppose that Bitcoin were to employ a transaction rate sufficient to process 150 million transactions per day and that Bitcoin's network delay were bounded below by empirical estimates given in Croman et al. (2016). Then, the following results hold:

(A) *Each block would correspond to a fork with over 99% probability and the blockchain would be in the state of a fork with over 99% probability.*

(B) *As a consequence, the expected time for transaction settlement would become prohibitive. More explicitly, the expected time for transaction settlement would exceed one year.*

Proposition 8 clarifies that the transaction rate necessary for Bitcoin to achieve VISA's US transaction volume (i.e., 150 million transactions per day) implies a frequency of forks such that user wait times become prohibitively lengthy irrespective of model preference parameters (i.e., $R_0, R_1, \alpha, \underline{c}, \overline{c}$). In turn, any reasonable model parameters are inconsistent with Bitcoin achieving such a transaction volume and thus Bitcoin faces a practical limit to adoption that renders it unlikely to compete with traditional payment systems.

To understand Proposition 8, note that Bitcoin achieving an increased transaction volume would require Bitcoin employing an increased transaction rate but an increased transaction rate would imply a higher fork probability (Proposition 8 (A)). The higher fork probability, in turn, would imply a higher expected wait time due to the need to achieve consensus on transaction settlement (Proposition 8 (B)). While particular preference parameters might be consistent with arbitrarily long settlement times (e.g., $R_0, R_1 = \infty$), we deem such model parameters as unreasonable because we do not consider it plausible that users would be willing to wait arbitrarily long for transaction settlement of casual payments.

More concretely, Eq. (5), which determines the fork probability, is central to Proposition 8. In particular, while current transaction rates for Bitcoin imply a near-zero fork probability, increasing Bitcoin's transaction rate to tolerate the demand of a traditional payment system would imply that most blocks would result in a fork. Consequently, most Bitcoin transactions would then be subjected to an elongated settlement process, thereby undermining adoption. We emphasize that a particular model-implied waiting time computation is not as relevant as the order of magnitude for wait times being unreasonably large whenever Bitcoin's transaction rate is expedited to tolerate large transaction demands.

To provide some practical context regarding the implications of persistent forks upon Bitcoin adoption, we turn to the only well-known example of a persistent Bitcoin fork. That fork demonstrates that persistent forks are a significant threat to widespread adoption in practice just as our model predicts. To provide more detail, a fork arose on the Bitcoin blockchain in March 2013 for technical reasons, but that fork was not resolved quickly so that it was persistent in a similar sense that forks generated in our model due to high transaction rates are persistent. In response to the fork, the largest cryptocurrency exchange at the time, Mt. Gox, suspended Bitcoin transactions, inducing a decline in Bitcoin usage. While Mt. Gox eventually restored Bitcoin transactions, the cause of the March 2013 fork was known to be idiosyncratic and thus not indicative of such a fork occurring in the future. In contrast, the forks that would arise if Bitcoin's transaction rate became too rapid are not idiosyncratic as they would arise regularly per our formal analysis. Mt. Gox's reaction to the March 2013 fork thus suggests that forks arising from an expedited Bitcoin transaction rate would undermine adoption more generally, which is consistent with our findings.[13]

5. Overcoming limited adoption

Although our results establish limited adoption for Bitcoin, our results do not imply that Bitcoin's adoption rate cannot be increased with centralization of Bitcoin mining. Moreover, our results do not imply that more recent economic designs of blockchains face limited adoption. We discuss these points, in turn, in Sections 5.1 and 5.2.

5.1. Bitcoin centralization

Lehar and Parlour (2020) and Cong et al. (2021a) highlight that Bitcoin mining markets are partially centralized in the sense that the majority of blocks are produced by a few mining pools. While such partial centralization does not preclude limited adoption (see Propositions 2 and 3), it does enable Bitcoin to achieve higher adoption rates for any finite level of transaction demand. We formalize this point with the following result:

Proposition 9. Partial Centralization of Mining Markets

Let π_*^C denote the adoption rate of Bitcoin if the network delay function is given by $\Delta_C(M)$. Let π_*^D denote the adoption rate of Bitcoin if the network delay function is given by $\Delta_D(M)$. We assume that $\Delta_C(M) \leq \Delta_D(M)$ for all M so that the former case reflects a (relatively) centralized mining market in which information propagates more quickly. Then, the adoption rate for the relatively centralized mining market exceeds that of the adoption rate for the relatively decentralized mining market (i.e., $\pi_*^C \geq \pi_*^D$).

Recall that M refers to the number of computer processors irrespective of the mining market structure. Since partial centralization of mining entails many such processors being controlled by the same entity, our model reflects partial centralization through a reduction in the network delay function (i.e., $\Delta_C(M) \leq \Delta_D(M)$ for all M). In that context, Proposition 9 demonstrates that a relatively centralized mining market implies a higher adoption rate than a more decentralized mining market. Intuitively, a relatively centralized mining market reduces not only the network delay but also the probability of a fork. In turn, a reduced fork probability implies a reduction in the expected settlement time for any transaction and thereby enables a higher equilibrium adoption rate.

5.2. Beyond Bitcoin

Our final result provides general context regarding overcoming limited adoption:

Proposition 10. Overcoming Limited Adoption

Suppose that the fork probability is given as follows:

$$\mathbb{P}(Fork) = p_F(\Lambda, \Delta(M))$$

where $p_F : \mathbb{R}_+ \times \mathbb{R}_+ \mapsto [0, 1]$ is an arbitrary function.

If the fork probability is bounded away from unity (i.e., $\sup_{\Lambda,\Delta} p_F(\Lambda, \Delta) < 1$), then widespread adoption (i.e., $\lim_{N\to\infty} \pi_* > 0$) can be obtained in equilibrium even with an arbitrarily large network (i.e., $\lim_{N\to\infty} M = \infty$).

Proposition 10 clarifies that limited adoption can be overcome if the fork probability is bounded away from unity. This result arises because the fork probability being bounded away from unity implies that the consensus wait time is bounded above and eventually decreases in the blockchain's transaction rate (see Lemma 7). In turn, a sufficiently large increase in the transaction rate reduces both consensus wait times and overall wait times, thereby enabling widespread adoption.

We conclude by discussing some prominent blockchain proposals that seek to improve upon Bitcoin. We discuss those proposals in the context of this paper's findings.

5.2.1. An expedited transaction rate

Several proposals aim to improve upon Bitcoin by employing a design identical to Bitcoin except with an expedited transaction rate. Such proposals are typically implemented either by increasing block sizes (e.g., Bitcoin Cash) or by increasing block rates (e.g., Litecoin). Our analysis indicates that such proposals do not succeed at overcoming limited adoption. In particular, Appendix A establishes that the fork probability approaches unity as the transaction rate diverges irrespective of whether the transaction rate diverges due to an increase in the block rate or an increase in the block size. Consequently, the consensus wait time becomes prohibitive as the transaction rate diverges irrespective of the implementation method for the increase in the transaction rate. In turn, expediting the transaction rate does not resolve the limited adoption problem as per Proposition 3.

While increasing the blockchain's transaction rate does not resolve the limited adoption problem, Proposition 10 indicates that limited adoption may be overcome by refining the blockchain's design to enable a high transaction rate without a high fork probability. Several blockchain proposals aim for such a refinement. The remainder of this section focuses on such proposals.

5.2.2. Bitcoin NG

Bitcoin NG, put forth by Eyal et al. (2015), confers authority to a single miner to add transactions to the blockchain for a period of time known as an *epoch*. This protocol differs from Bitcoin in that Bitcoin confers such authority only for a single block. The described modification enables Bitcoin NG to achieve a lower fork probability because a fork cannot arise within an epoch once the entire network has learned which particular miner has the authority to add blocks during the epoch.

Bitcoin NG confers authority to a miner to add transactions in the same manner that Bitcoin selects a block to be added to the blockchain. In particular, in both cases, a miner must create a block which solves a computationally intensive puzzle to receive the authority to add transactions. In Bitcoin's case, the transactions that can be added to the blockchain must be included directly on the block

[13] For additional details regarding the March 2013 fork, the interested reader may consult Biais et al. (2019) or Saleh (2021).

that solves the puzzle. In contrast, in Bitcoin NG's case, the block that solves the puzzle identifies a miner who may add transactions to the blockchain for the duration of the epoch, and no other miner may add transactions during the epoch. Once the epoch concludes, Bitcoin NG confers authority to another miner to add transactions for the subsequent epoch in the same manner as for the previous epoch.

Intuitively, Bitcoin NG achieves a reduction in the fork probability by implementing a temporary centralization of authority. More explicitly, each epoch corresponds to a period in which a single miner has a monopoly with regard to adding transactions to the blockchain. As a consequence, a fork cannot arise within an epoch for the same reason that a fork would not arise in general in a centralized setting. It is noteworthy that Bitcoin NG may maintain a fork probability bounded away from unity even when expanding its transaction rate by extending the duration of each epoch.

5.2.3. Modern proof-of-stake protocols

The previously referenced concept of dividing time into epochs and pre-specifying authority to add transactions within the epoch has been used in many recent blockchain proposals. A key distinguishing factor between some of those recent proposals and Bitcoin NG is that recent proposals generally do not confer authority on the basis of computational puzzles. Rather, most recent proposals confer such authority on the basis of lotteries over outstanding cryptocurrency units (or a subset of those units) with the lottery winners receiving the authority to add blocks to the blockchain and the blocks including transactions. Such recent proposals are referred to as employing a *Proof-of-Stake (PoS)* protocol because an agent's likelihood of receiving the authority to add blocks depends upon her *stake* where stake refers to cryptocurrency holdings.[14]

The particular concept of having a single agent determine all transactions within an epoch has been employed by some PoS blockchains (see, e.g., Pass and Shi, 2018), but many others employ a further modification that entails dividing each epoch into *slots* where each slot corresponds to a single block. In such a case, each slot is assigned to an agent based on independent lotteries, and all lotteries for slots within a particular epoch occur at the beginning of that epoch. This process of specifying which agent may add a block in each slot of the epoch keeps the fork probability low because of the lack of ambiguity regarding which agent may add a block in a particular slot. Moreover, the number of slots within each epoch may be increased when increasing the transaction rate to keep the fork probability bounded away from unity.

5.2.4. Permissioned blockchains

Another method to enable high transaction rates without inducing a high fork probability is to specify the underlying blockchain as a permissioned blockchain. A permissioned blockchain differs from Bitcoin and PoS blockchains in that the set of agents who may participate in the process of creating blocks is set in an exogenous fashion. Moreover, this set is typically kept to a small number, and an efficient process is specified for the agents within the set to arrive at consensus on blocks.

One process frequently used for generating consensus in a permissioned blockchain is Practical Byzantine Fault Tolerance (PBFT). PBFT, introduced by Castro et al. (1999), entails one agent being designated as the leader where only the leader can propose new blocks. Consequently, a permissioned blockchain with PBFT can operate at high transaction rates while avoiding a high fork probability.

6. Conclusion

Bitcoin was created with the ambition of becoming a widely-adopted decentralized payment system. To date, Bitcoin has fallen short of that goal. Our paper examines Bitcoin's goal in the context of its design and finds the former incompatible with the latter. In particular, we find that limited adoption is an equilibrium outcome for Bitcoin.

Nonetheless, we emphasize that our work does not imply limited adoption universally across all blockchains. Rather, our results apply only to Bitcoin and similar blockchains, thereby highlighting the need for economic analysis of blockchains other than Bitcoin. As discussed within Section 5.2, some blockchain proposals that show promise to overcome limited adoption include Bitcoin NG, modern Proof-of-Stake protocols and Permissioned blockchains.[15] We hope that researchers will extend our framework to formally examine those ideas in the future.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

Ron Kaniel was the editor for this article. We thank the editor and two anonymous referees for many helpful suggestions. We also thank Anup Agrawal, Yakov Amihud, Daniel Andrei, Bruno Biais, Jaroslav Borovicka, Matthieu Bouvard, Agostino Capponi, Lin William Cong, Kathleen DeRose, Sean Foley, Vishal Gaur, Thomas George, Manasa Gopal, Hanna Halaburda, Rick Harris, Iftekhar Hasan, Joel Hasbrouck, Craig Holden, Sabrina Howell, Gur Huberman, Felix Irresberger, Ari Juels, Steven Kou, Jongsub Lee, Doron Levit, Jiasun Li, Tao Li, Ye Li, Laura Xiaolei Liu, Evgeny Lyandres, Katya Malinova, Bill Marcum, David Musto, Shunya Noda, Maureen O'Hara, Andreas Park, Christine Parlour, Ajay Patel, Thomas Rivera, Alberto Rossi, Bryan Routledge, Ville Savolainen, Zhan Shi, Chester Spatt, Deon Strickland, Raghu Sundaram, Charles Trzcinka, Gerry Tsoukalas, Larry Wall, Baolian Wang, Chaojun Wang, Warren Weber, Danxia

[14] A discussion of PoS is beyond the scope of this paper. The interested reader may consult Saleh (2021) for details.

[15] For technical details on such proposals and other potential solutions for limited adoption, we direct readers to Zhou et al. (2020).

Xie, Baozhong Yang, David Yermack and Zhen Zhou, as well as seminar participants at Georgetown University, Indiana University, NYU Stern, Peking University, Tsinghua PBC School of Finance, Tsinghua School of Social Sciences, University of Florida, University of Georgia, University of Houston, Wake Forest University and conference participants at the 2019 Conference on Financial Economics and Accounting, the 2020 American Finance Association meeting, the 2020 Midwest Finance Association meeting, the 2020 European Finance Association meeting and the 2020 Tokenomics Conference for valuable comments.

Appendix A. Fork probability

As explained in Section 2.3, a valid block produced by some Miner i does not correspond to a fork if no blocks inconsistent with it are produced. Therefore:

$$\mathbb{P}(Fork) = 1 - \mathbb{P}(\bigcap_j \{Miner\ j\ does\ not\ produce\ a\ valid\ inconsistent\ block\}) \tag{A.1}$$

Recall that Miner j produces a valid block inconsistent with Miner i's block if and only if Miner j produces a valid block before receiving news of Miner i's block. Accordingly, for Miner j's next valid block to be consistent with Miner i's valid block, Miner j must not generate a valid block in the time that Miner i takes to communicate her block to Miner j. Decker and Wattenhofer (2013) demonstrate that this time, also known as the network delay between Miners i and j, depends upon the amount of information being sent and is approximately linear in the size of information being sent. Thus, letting σ denote the block size (i.e., number of transactions per block) and $\Delta_{i,j}$ denote the network delay between Miners i and j for a block with one transaction, we have that:

$$Network\ Delay\ Between\ Miners\ i\ and\ j = \sigma \times \Delta_{i,j} \tag{A.2}$$

Further, letting X_j denote the time until Miner j produces her next valid block (starting from the time at which Miner i produces a valid block), we also have that:

$$\{Miner\ j\ does\ not\ produce\ a\ valid\ inconsistent\ block\} = \{X_j > \sigma \times \Delta_{i,j}\} \tag{A.3}$$

It is well known that each miner's block production process is independent (see, e.g., Narayanan et al., 2016) so that Eqs. (A.1)–(A.3) imply:

$$\mathbb{P}(Fork) = 1 - \prod_j \mathbb{P}(\{X_j > \sigma \times \Delta_{i,j}\}) \tag{A.4}$$

As discussed within Sections 2.2 and 2.3, each miner produces valid blocks according to a Poisson process and each miner corresponds to a computer processor of comparable hashing power. Thus, X_j is an exponential random variable with some parameter $\lambda > 0$ that denotes the rate at which each miner produces valid blocks, and Eq. (A.4) becomes:

$$\mathbb{P}(Fork) = 1 - \prod_j e^{-\lambda \times \sigma \times \Delta_{i,j}} \tag{A.5}$$

Then, after some algebra, we have that:

$$\mathbb{P}(Fork) = 1 - e^{-\lambda \times M \times \sigma \times \frac{1}{M} \sum_j \Delta_{i,j}} \tag{A.6}$$

Recall that λ denotes the block rate for an individual miner and M denotes the total number of miners so that $\rho \equiv \lambda \times M$ denotes the block rate for the entire mining network. Additionally, since σ denotes the number of transactions per block, $\Lambda \equiv \rho \times \sigma = \lambda \times M \times \sigma$ equals the blockchain's transaction rate. Finally, as $\Delta_{i,j}$ denotes the network delay between Miners i and j for a normalized single-transaction block, $\Delta(M) \equiv \frac{1}{M} \sum_j \Delta_{i,j}$ denotes the average network delay for a normalized single-transaction block.[16] Then, a simple re-writing of Eq. (A.6) delivers Eq. (5):

$$\mathbb{P}(Fork) = 1 - e^{-\Lambda \Delta(M)} \tag{A.7}$$

Equivalence between Block Rates, ρ, and Block Sizes, σ

Our results establish an equivalence between modifying block rates, ρ, and modifying block sizes, σ. In particular, recall that $\Lambda = \rho \times \sigma$ so that Eq. (A.7) implies:

$$\mathbb{P}(Fork) = 1 - e^{-\rho \times \sigma \times \Delta(M)} \tag{A.8}$$

Formally, the block rate, ρ, and the block size, σ, enter symmetrically within Eq. (A.8) so that a change in the former produces identical implications as a change in the latter. Accordingly, we may study implications of varying the blockchain transaction rate, $\Lambda = \rho \times \sigma$, upon fork probabilities without specific attention to whether the changes in the transaction rate are achieved by modifying the block rate, ρ, or the block size, σ.

To provide some intuition for this point, we remind the reader that a fork arises when some Miner j produces a valid block before receiving news of the prior valid block by Miner i. Thus, intuitively, a fork arises for one of two reasons: either Miner j produces a valid block too quickly, or Miner i's block requires too long to communicate to the network. Increasing the block rate, ρ, makes a fork more likely due to the former reason, whereas increasing the block size, σ, makes the fork more likely due to the latter reason. In particular, a faster block rate implies that each miner produces blocks at a faster rate (i.e., $\rho \uparrow \Rightarrow \lambda = \frac{\rho}{M} \uparrow$) whereas a larger block size, σ, implies that Miner i's block takes longer to communicate (i.e., $\sigma \uparrow \Rightarrow \sigma \times \Delta_{i,j} \uparrow$). In the former case, the fork becomes more likely because the likelihood that some Miner j produces a valid block too quickly increases; in the latter case, the fork becomes more likely because the time necessary for Miner i to communicate with each Miner $j \neq i$ elongates.

Appendix B. CTMC Blockchain model

We model the blockchain as a Continuous Time Markov Chain (CTMC), $\{X_t\}_{t \geq 0}$, with states $x \in X \equiv \{0, 1, \ldots, b\}$. In our model, any state $x < b$ corresponds to a state in which the blockchain is in the midst of a fork whereas the state $x = b$ corresponds to the blockchain being in a state of consensus. Recall that from a state of consensus (i.e., $x = b$),

[16] As the Bitcoin network is not supposed to favor any participant relative to any other participant, we impose symmetry and drop the i subscript (i.e., $\Delta(M) = \Delta_i(M) \equiv \frac{1}{M} \sum_j \Delta_{i,j}$).

the blockchain enters a fork if there are multiple blocks generated at a given height. We denote the blockchain state immediately after there is a disagreement on the most recent block by $x = 0 < b$. As discussed in Section 2.3, regaining consensus requires agreement on b consecutive blocks, and we keep track of this transition through the blockchain's state by incrementing the blockchain state by one with each consecutive block on which there is agreement until the blockchain regains consensus (i.e., $x = b$) at which point the state remains at $x = b$ until there is disagreement on a block. As at any other time, if there is a disagreement on a block during the aforementioned transition period or after regaining consensus, the blockchain state then changes to $x = 0$.

Formally, the CTMC rate matrix, $Q \in \mathbb{R}^{X\times X}$, characterizes our model. For exposition, we define $p(x, y) = 1 - e^{-xy}$ and abuse notation by setting $p \equiv p(\Lambda, \Delta) = 1 - e^{-\Lambda\Delta} \in (0, 1)$. Note that p corresponds to the fork probability (see Eq. (5)). Then, since blocks arrive at rate Λ and only the states $x = 0$ and $x = b$ can transition back to themselves, we have that $\forall x \in X/\{0, b\} : Q_{x,x} = -\Lambda$. Moreover, since there is disagreement over any block with probability p and the blockchain transitions to state $x = 0$ upon such disagreement, we have that $\forall x \in X/\{0\} : Q_{x,0} = \Lambda p$. Similarly, since the state of the blockchain increments from x to $x + 1$ until $x = b$ whenever there is agreement on a block (which occurs with probability $1 - p$ for any given block), we have that $\forall x \in X/\{b\} : Q_{x,x+1} = \Lambda(1 - p)$. Finally, trivially, we have that $Q_{b,b} = -\Lambda p$, $Q_{0,0} = -\Lambda(1 - p)$ and all other entries of Q equal 0.

Lemma 1. Stationary Distribution

$\{\pi_x\}_{x\in X}$ corresponds to the unique stationary distribution with $\forall x < b : \pi_x = p(1 - p)^x$ and $\pi_b = (1 - p)^b$

Proof. Any stationary distribution, $\tilde{\pi} \in \mathbb{R}^X$, must satisfy $\tilde{\pi} Q = 0$. The result follows from algebra. □

For exposition, we uniformize our CTMC. We let $\{Y_t\}_{t\in\mathbb{N}}$ denote the associated Discrete Time Markov Chain (DTMC) and $P \in \mathbb{R}^{X\times X}$ denote the associated transition matrix. Then, $X_t = Y_{N(t)}$ with $\{N(t)\}_{t\geq 0}$ being a Poisson Process with rate Λ.

Lemma 2. Consensus Wait Times

We define $T_b \equiv \inf\{t \in \mathbb{N} : Y_t = b\}$. Then, the expected block heights until fork resolution, $s_x = \mathbb{E}[T_b|Y_0 = x]$, conditional upon initial state, $x \in X$, satisfies $\forall x \in X : s_x = (1 + s_0 p)\frac{1-(1-p)^{b-x}}{p} \quad \forall x \in X$ so that $s_0 = \frac{1-(1-p)^b}{p(1-p)^b}$.

Proof. We prove the result by induction. $s_{k-j} = (1 + s_0 p)\sum_{i=0}^{j-1}(1 - p)^i$ holds for $j = 1$ by definition. Then, $s_{k-(j+1)} = 1 + (1 - p)s_{k-j} + ps_0 = (1 + s_0 p)\sum_{i=0}^{(j+1)-1}(1 - p)^i$ with the last equality following from the inductive hypothesis. The conclusion then follows from algebra. □

Subsequently, we provide results useful for establishing results within the body of our manuscript, which are subsequently proved in Appendix C.

Lemma 3. Monotone Consensus Wait Times

$\forall x \in X/\{b\} : s_x > s_{x+1} \geq 0$

Proof. We prove the result by induction. By definition, $\forall x \in X/\{b\} : s_x = 1 + (1 - p)s_{x+1} + ps_0$ so that $s_0 > s_1$ follows by taking $x = 0$. Then, by induction, $s_x = 1 + (1 - p)s_{x+1} + ps_0 > 1 + (1 - p)s_{x+1} + ps_x$ which implies $s_x > s_{x+1}$ as desired. $\forall x \in X/\{b\} : s_{x+1} \geq 0$ follows from $s_b = 0$. □

Hereafter, we define $\forall x \in X : s_x(\Lambda, \Delta) \equiv s_x(p) \equiv s_x(p(\Lambda, \Delta))$ and abuse notation by using s_x to mean the multivariate function. Similarly, we define $\forall x \in X : \pi_x(\Lambda, \Delta) \equiv \pi_x(p) \equiv \pi_x(p(\Lambda, \Delta))$ and abuse notation by using π_x to mean the multivariate function.

Lemma 4. Monotone Consensus Wait Times Derivatives

$\forall x \in X/\{b\} : \frac{ds_x}{dp} \equiv \frac{d}{dp}[s_x(p)] > \frac{ds_{x+1}}{dp} \equiv \frac{d}{dp}[s_{x+1}(p)] \geq 0$

Proof. We prove the result by induction. By definition, $\forall x \in X/\{b\} : s_x = 1 + (1 - p)s_{x+1} + ps_0$ so that $s_0 = \frac{1}{1-p} + s_1$ and thus $\frac{ds_0}{dp} = \frac{1}{(1-p)^2} + \frac{ds_1}{dp} > \frac{ds_1}{dp}$. Then, $s_x = 1 + (1 - p)s_{x+1} + ps_0$ implies $\frac{ds_x}{dp} = (1 - p)\frac{ds_{x+1}}{dp} - s_{x+1} + p\frac{ds_0}{dp} + s_0$. Then, Lemma 3 gives that $s_0 > s_{x+1}$ and the inductive hypothesis gives that $\frac{ds_0)}{dp} > \frac{ds_x}{dp}$ so that $(1 - p)\frac{ds_{x+1}}{dp} - s_{x+1} + p\frac{ds_0}{dp} + s_0 > (1 - p)\frac{ds_{x+1}}{dp} + p\frac{ds_x}{dp}$ so that $\frac{ds_x}{dp} > (1 - p)\frac{ds_{x+1}}{dp} + p\frac{ds_x}{dp}$. The last equation further implies $\frac{ds_x}{dp} > \frac{ds_{x+1}}{dp}$, which provides the inductive step and thereby establishes $\frac{ds_x}{dp} > \frac{ds_{x+1}}{dp}$ for all $x \in X/\{b\}$. To complete the proof, we must demonstrate that $\frac{ds_{x+1}}{dp} \geq 0$ for all $x \in X/\{b\}$. This follows immediately from $s_b = 0$, which itself follows from the definition of s_b. More precisely, since we already have $\frac{ds_x}{dp} > \frac{ds_{x+1}}{dp}$ for all $x \in X/\{b\}$, then, for all $x \in X/\{b\}$, $\frac{ds_{x+1}}{dp} \geq \frac{ds_b}{dp} = 0$. □

Lemma 5. Monotone Consensus Wait Times Derivatives II

$\forall x \in X/\{b\} : \frac{\partial s_x}{\partial \Lambda} > \frac{\partial s_{x+1}}{\partial \Lambda} \geq 0, \frac{\partial s_x}{\partial \Delta} > \frac{\partial s_{x+1}}{\partial \Delta} \geq 0$

Proof. For all $x \in X/\{b\}$, $\frac{\partial s_x}{\partial \Lambda} = \frac{ds_x}{dp}\frac{\partial p}{\partial \Lambda} = \frac{ds_x}{dp}\Delta e^{-\Lambda\Delta}$. In turn:

$$\forall x \in X/\{b\} : \frac{\partial s_x}{\partial \Lambda} > \frac{\partial s_{x+1}}{\partial \Lambda} \geq 0 \iff \frac{ds_x}{dp} > \frac{ds_{x+1}}{dp} \geq 0$$

so that $\forall x \in X/\{b\} : \frac{\partial s_x}{\partial \Lambda} > \frac{\partial s_{x+1}}{\partial \Lambda} \geq 0$ follows from Lemma 5.

The proof for the second half of the lemma is similar. More explicitly, for all $x \in X/\{b\}$, $\frac{\partial s_x}{\partial \Delta} = \frac{ds_x}{dp}\frac{\partial p}{\partial \Delta} = \frac{ds_x}{dp}\Lambda e^{-\Lambda\Delta}$. In turn:

$$\forall x \in X/\{b\} : \frac{\partial s_x}{\partial \Delta} > \frac{\partial s_{x+1}}{\partial \Delta} \geq 0 \iff \frac{ds_x}{dp} > \frac{ds_{x+1}}{dp} \geq 0$$

and thus $\forall x \in X/\{b\} : \frac{\partial s_x}{\partial \Delta} > \frac{\partial s_{x+1}}{\partial \Delta} \geq 0$ also follows from Lemma 5. □

We define $\tilde{\tau} \equiv \mathbb{E}[T_b]$ as the expected number of blocks until fork resolution under the stationary distribution. We further define $\tau \equiv \mathbb{E}[\sum_{t=1}^{T_b} A_t]$ as the expected fork resolution time under the stationary distribution with $\{A_t\}_{t=1}^{\infty}$ independent and exponentially distributed. Note that the stationary distribution is given by $\{\pi_x\}_{x\in X}$, which is given explicitly in Lemma 1. Note also that $Z_i \overset{d}{=} \sum_{t=1}^{T_b} A_t$ where Z_i denotes the expected fork resolution time for User i, and that the distribution for all Z_i are identical because we initialize our model with the stationary distribution.

Note that $\tau \equiv \mathbb{E}[\sum_{t=1}^{T_b} A_t] = \mathbb{E}[A_1] \times \mathbb{E}[T_b] = \frac{1}{\Lambda} \times \tilde{\tau}$, because $\{A_t\}_{t=1}^{\infty}$ is an i.i.d sequence. More explicitly, $\tilde{\tau} = \tilde{\tau}(p) \equiv \sum_{x \in X} s_x(p)\pi_x(p)$, whereas $\tau = \tau(p, \Lambda) \equiv \sum_{x \in X} \frac{s_x(p)}{\Lambda}\pi_x(p)$.

Lemma 6. $\tilde{\tau}$ Increases in p

Let $p, p' \in (0, 1)$ such that $p \leq p'$. Then, $\tilde{\tau}(p) \leq \tilde{\tau}(p')$

Proof. Recall that $\tilde{\tau}(p) = \sum_{x \in X} s_x(p)\pi_x(p)$ by definition. Then, since Lemma 4 implies $s_x(p) \leq s_x(p')$, we have that $\tilde{\tau}(p) = \sum_{x \in X} s_x(p)\pi_x(p) \leq \sum_{x \in X} s_x(p')\pi_x(p)$. Lemma 1 implies that the stationary distribution characterized by p first-order stochastically dominates that characterized by p', whereas Lemma 2 implies that s_x is a decreasing function of x; these two results collectively imply $\sum_{x \in X} s_x(p')\pi_x(p) \leq \sum_{x \in X} s_x(p')\pi_x(p')$.[17] In turn, $\tilde{\tau}(p) \leq \sum_{x \in X} s_x(p')\pi_x(p) \leq \sum_{x \in X} s_x(p')\pi_x(p') = \tilde{\tau}(p')$ as desired. □

Lemma 7. τ vanishes in Λ if fork probability bounded away from unity

Suppose that the fork probability is given by an arbitrary function $p_F : \mathbb{R}_+ \times \mathbb{R}_+ \mapsto [0, 1]$ such that $\sup\limits_{\Lambda,\Delta} p_F(\Lambda, \Delta) < 1$. Then, for any sequence $\{\Lambda_N, \Delta_N\}_{N=1}^{\infty}$ such that $\lim\limits_{N\to\infty} \Lambda_N = \infty$, we have that $\lim\limits_{N\to\infty} \tau(p_F(\Lambda_N, \Delta_N), \Lambda_N) = 0$.

Proof. Lemma 6 implies that $\tilde{\tau}(p_F(\Lambda_N, \Delta_N)) \leq \tilde{\tau}(\sup\limits_{\Lambda,\Delta} p_F(\Lambda, \Delta)) < \infty$ for all N so that $\sup\limits_{N} \tilde{\tau}(p_F(\Lambda_N, \Delta_N)) \leq \tilde{\tau}(\sup\limits_{\Lambda,\Delta} p_F(\Lambda, \Delta)) < \infty$. Then, $\tau(p_F(\Lambda_N, \Delta_N)), \Lambda_N) = \frac{1}{\Lambda_N} \times \tilde{\tau}(p_F(\Lambda_N, \Delta_N)) \leq \frac{1}{\Lambda_N} \times \tilde{\tau}(\sup\limits_{\Lambda,\Delta} p_F(\Lambda, \Delta))$ for any N implies that $\limsup\limits_{N\to\infty} \tau(p_F(\Lambda_N, \Delta_N), \Lambda_N) \leq \limsup\limits_{N\to\infty} \Big(\frac{1}{\Lambda_N} \times \tilde{\tau}(\sup\limits_{\Lambda,\Delta} p_F(\Lambda, \Delta))\Big) = \lim\limits_{N\to\infty} \left(\frac{1}{\Lambda_N}\right) \times \tilde{\tau}(\sup\limits_{\Lambda,\Delta} p_F(\Lambda, \Delta)) = 0$. Finally, recall that τ is defined as the expectation of a non-negative random variable so that $\liminf\limits_{N\to\infty} \tau(p_F(\Lambda_N, \Delta_N), \Lambda_N) \geq 0$ holds trivially and thus $\lim\limits_{N\to\infty} \tau(p_F(\Lambda_N, \Delta_N), \Lambda_N) = 0$ as desired. □

We define $\tau(\Lambda, \Delta) \equiv \tau(p(\Lambda, \Delta), \Lambda)$. Recall that $p(\Lambda, \Delta) = 1 - e^{-\Lambda\Delta}$ which is the fork probability function for Bitcoin (see Appendix A). In turn, $\tau(\Lambda, \Delta)$ corresponds specifically to Bitcoin's consensus wait time. When examining more general settings (e.g., Section 5.2, Proposition 10 and Lemma 7), we explicitly acknowledge the underlying fork probability function (e.g., $\tau = \tau(p_F) = \tau(p_F(\Lambda, \Delta), \Lambda)$ for fork probability function p_F).

Lemma 8. Lower Bound for τ

$\tau(\Lambda, \Delta) \geq \Delta \frac{e^{\Lambda\Delta} - 1}{\Lambda\Delta}$

Proof. $\tau(\Lambda, \Delta) \geq \Delta \frac{s_0(\Lambda, \Delta)}{\Lambda\Delta} \pi_0(\Lambda, \Delta) = \Delta \frac{e^{\Lambda\Delta b} - 1}{\Lambda\Delta} \geq \Delta \frac{e^{\Lambda\Delta} - 1}{\Lambda\Delta}$ as desired. □

We define $\Psi(\Lambda, \Delta) \equiv \tau(\Lambda, \Delta) + \frac{1}{\Lambda} = \tau(p(\Lambda, \Delta), \Lambda) + \frac{1}{\Lambda}$ which equates with the expected wait time for the marginal user (i.e., Type $c_i = c_*$). Unless explicitly stated otherwise (e.g., Proposition 10), we use $p(\Lambda, \Delta) = 1 - e^{-\Lambda\Delta}$, which is Bitcoin's fork probability function.

Lemma 9. Ψ reduces in Centralization

Let $\Delta_C : \mathbb{R}_+ \mapsto \mathbb{R}_+$ and $\Delta_D : \mathbb{R}_+ \mapsto \mathbb{R}_+$ denote network delay functions such that $\Delta_C(M) \leq \Delta_D(M)$ for all M. Then, $\Psi(\Lambda, \Delta_C(M)) \leq \Psi(\Lambda, \Delta_D(M))$ for all $\Lambda, M \geq 0$.

Proof. By definition, $\Psi(\Lambda, \Delta_i(M)) = \tau(p(\Lambda, \Delta_i(M))) + \frac{1}{\Lambda} = \frac{1}{\Lambda} \cdot \tilde{\tau}(p(\Lambda, \Delta_i(M))) + \frac{1}{\Lambda}$ for $i \in \{C, D\}$. Then, $p(\Lambda, \Delta) = 1 - e^{-\Lambda\Delta}$ implies that $p(\Lambda, \Delta_C(M)) \leq p(\Lambda, \Delta_D(M))$ so that Lemma 6 implies $\tilde{\tau}(p(\Lambda, \Delta_C(M))) \leq \tilde{\tau}(p(\Lambda, \Delta_D(M))$. In turn, $\Psi(\Lambda, \Delta_C(M)) = \frac{1}{\Lambda} \cdot \tilde{\tau}(p(\Lambda, \Delta_C(M))) + \frac{1}{\Lambda} \leq \frac{1}{\Lambda} \cdot \tilde{\tau}(p(\Lambda, \Delta_D(M))) + \frac{1}{\Lambda} = \Psi(\Lambda, \Delta_D(M))$ as desired. □

Lemma 10. Increasing Wait Time in M

$\forall M' > M \geq 0 : \Psi(\Lambda, \Delta(M')) - \Psi(\Lambda, \Delta(M)) = \tau(\Lambda, \Delta(M')) - \tau(\Lambda, \Delta(M)) > 0$

Proof.

$$\begin{aligned} &\Psi(\Lambda, \Delta(M')) - \Psi(\Lambda, \Delta(M)) \\ &= \tau(\Lambda, \Delta(M')) - \tau(\Lambda, \Delta(M)) \\ &= \sum_{x \in X}\Big\{\frac{s_x(\Lambda, \Delta(M'))}{\Lambda}\pi_x(\Lambda, \Delta(M')) - \frac{s_x(\Lambda, \Delta(M))}{\Lambda}\pi_x(\Lambda, \Delta(M))\Big\} \\ &\geq \sum_{x \in X} \frac{s_x(\Lambda, \Delta(M')) - s_x(\Lambda, \Delta(M))}{\Lambda}\pi_x(\Lambda, \Delta(M)) \\ &= \sum_{x \in X} \frac{1}{\Lambda} \int_{M}^{M'} \frac{\partial s_x}{\partial \Delta}\Big|_{\Delta = \Delta(m)} \Delta'(m) dm \; \pi_x(\Lambda, \Delta(M)) \\ &> 0 \end{aligned}$$

□

Lemma 11. Zero Wait

$\tau(\Lambda, 0) = 0$

Proof. $\tau(\Lambda, 0) = s_k(\Lambda, 0) = 0$ □

Appendix C. Proofs for results in main text

Appendix C.1 derives Proposition 1, which establishes equilibrium existence. Appendix C.2 then derives preliminary lemmas that are necessary for proving the results stated within Sections 3–5. Our proofs of Propositions 2 and 3 rely upon Propositions 6 and 7 respectively, so we derive our results in this Appendix in a different order than that which the results are stated in the manuscript. More explicitly, we first derive the results from Section 4 in Appendix C.3 and then derive all other results in Appendix C.4. Our ordering of proofs within this Appendix ensures that each proof relies only upon results derived earlier within the Appendices.

C1. Proof of Proposition 1

Proof. For coherence of our discussion, we must specify an initial distribution for our Blockchain CTMC model. We specify that distribution as the stationary distribution as

[17] To see this point, note that $\sum_{x \in X} s_x(p')\pi_x(p)$ and $\sum_{x \in X} s_x(p')\pi_x(p')$ each correspond to expectations of the same random variable that takes on values $\{s_x(p')\}_{x \in X}$. For each $x \in X$, $s_x(p')$ occurs with probability $\pi_x(p)$ in the first case and with probability $\pi_x(p')$ in the second case. Crucially, as $s_x(p')$ decreases in x, the expectation is higher when taken with respect to the distribution which is smaller in the sense of first-order stochastic dominance (i.e., $\sum_{x \in X} s_x(p')\pi_x(p) \leq \sum_{x \in X} s_x(p')\pi_x(p')$).

derived in Lemma 1. The interested reader may consult Appendix B for additional details.

We proceed as follows: first, we assume that users take the equilibrium objects c_* and M as given and establish that (A) gives the equilibrium fee function in that context. Then, we demonstrate that (B)–(D) must hold. Finally, we demonstrate existence of c_* and M that satisfy (B)–(D), thereby completing the proof.

Establishing (A) given c_* and M

Definition 1 (iii) requires that the equilibrium fee function, ϕ, satisfies:

$$\phi(c_i) = \underset{f\geq 0}{\arg\max}\ R_1 \cdot (\pi_* N)^{\alpha} + R_0 - c_i \cdot \mathbb{E}[W(f, f_{-i})] - f \tag{C.1}$$

for $c_i \leq c_*$. Then, since transactions are processed in descending fee order and blocks are unit-sized, Definition 1 (iv) implies:

$$\mathbb{E}[W(f, f_{-i})] = \frac{1}{\Lambda} \times \mathbb{E}[\sum_{j:j\neq i} \mathcal{I}\{f_j > f\}\ ] + \mathbb{E}[Z_i] \tag{C.2}$$

where the first term on the right-hand side represents the wait due to higher-priority users and the second term on the right-hand side represents the stationary expected wait time due to the need for miners to attain consensus.

Per Definition 1 (iii), each user who does not adopt Bitcoin (i.e., any User j such that $c_j > c_*$) optimally pays zero fees. Consequently, $f_j > f \geq 0$ implies $c_j \leq c_*$ and thus Eq. (C.2) can be re-written as:

$$\mathbb{E}[W(f, f_{-i})] = \frac{1}{\Lambda} \times \mathbb{E}[\sum_{j:j\neq i} \mathcal{I}\{c_* \geq c_j,\ \ f_j > f\}\ ] + \mathbb{E}[Z_i] \tag{C.3}$$

Note that Definition 1 (ii) imposes that each user anticipates that adopting users (i.e., any User j such that $c_j \in [\underline{c}, c_*]$) select fees according to the equilibrium fee function, ϕ. As a consequence, $f_j = \phi(c_j)$ for all j so that Eq. (C.3) becomes:

$$\mathbb{E}[W(f, f_{-i})] = \frac{1}{\Lambda} \times \mathbb{E}[\sum_{j:j\neq i} \mathcal{I}\{c_* \geq c_j,\ \ \phi(c_j) > f\}\ ] + \mathbb{E}[Z_i] \tag{C.4}$$

Then, using $\{c_j\}_{j=1}^{N}$ being i.i.d yields:

$$\mathbb{E}[W(f, f_{-i})] = \mathbb{E}[W(f, \phi(c_{-i})] = \frac{N-1}{\Lambda} \times \mathbb{P}\{c_* \geq c_j,\ \ \phi(c_j) > f\} + \mathbb{E}[Z_i] \tag{C.5}$$

We follow prior literature and restrict ourselves to ϕ being strictly increasing over the set of adopting users. Hence, the inverse of ϕ, ϕ^{-1}, is well-defined and Eq. (C.5) becomes:

$$\begin{aligned}\mathbb{E}[W(f, f_{-i})] &= \mathbb{E}[W(f, \phi(c_{-i})] \\ &= \frac{N-1}{\Lambda} \times \mathbb{P}\{c_* > c_j > \phi^{-1}(f)\} + +\mathbb{E}[Z_i]\end{aligned} \tag{C.6}$$

Since $c_j \sim U[\underline{c}, \bar{c}]$, Eq. (C.6) simplifies to:

$$\begin{aligned}\mathbb{E}[W(f, f_{-i})] &= \mathbb{E}[W(f, \phi(c_{-i})] \\ &= \frac{N-1}{\Lambda} \times \max\left\{\frac{c_* - \phi^{-1}(f)}{\bar{c} - \underline{c}}, 0\right\} + \mathbb{E}[Z_i]\end{aligned} \tag{C.7}$$

Applying Eq. (C.7) to Eq. (C.1) then yields:

$$\phi(c_i) = \underset{f\geq 0}{\arg\max}\ \Gamma - \frac{c_i \cdot (N-1)}{\Lambda} \times \max\{\frac{c_* - \phi^{-1}(f)}{\bar{c} - \underline{c}}, 0\} - f \tag{C.8}$$

where $\Gamma = R_1 \cdot (\pi_* N)^{\alpha} + R_0 - c_i \cdot \mathbb{E}[Z_i]$ does not depend upon User i's fee choice. Note that paying $f_i > \phi(c_*)$ is dominated by paying $f_i = \phi(c_*)$ because paying $f_i = \phi(c_*)$ ensures a user the highest priority with probability one; in particular, paying $f_i > \phi(c_*)$ does not reduce wait time relative to $f_i = \phi(c_*)$ and thus only reduces user utility relative to $f_i = \phi(c_*)$ because $f_i > \phi(c_*)$ entails higher disutility from the higher fee payment. As a consequence, without loss of generality, we can restrict the fee optimization problem to $f \in [0, \phi(c_*)]$ and Eq. (C.8) thereby becomes:

$$\phi(c_i) = \underset{f\in[0,\phi(c_*)]}{\arg\max}\ \Gamma - \frac{c_i \cdot (N-1)}{\Lambda} \times \frac{c_* - \phi^{-1}(f)}{\bar{c} - \underline{c}} - f \tag{C.9}$$

Then, taking the first order condition yields:

$$\frac{c_i \cdot (N-1)}{\Lambda \cdot (\bar{c} - \underline{c})} \times \frac{1}{\phi'(\phi^{-1}(f_i))} - 1 = 0 \tag{C.10}$$

where f_i is User i's optimal fee. In equilibrium, per Definition 1 (ii), we must have $f_i = \phi(c_i)$ so that Eq. (C.10) then becomes:

$$\frac{c_i \cdot (N-1)}{\Lambda \cdot (\bar{c} - \underline{c})} \times \frac{1}{\phi'(c_i)} - 1 = 0 \tag{C.11}$$

Note that Eq. (C.11) represents a differential equation that the equilibrium fee function must satisfy. In particular, after some algebra, Eq. (C.11) becomes:

$$\phi'(c_i) = \frac{c_i \cdot (N-1)}{\Lambda \cdot (\bar{c} - \underline{c})} \tag{C.12}$$

Note that $\phi(\underline{c}) = 0$ must hold in any equilibrium where ϕ is strictly increasing over $[\underline{c}, \bar{c}]$. This is because ϕ strictly increasing over $[\underline{c}, \bar{c}]$ implies that any User j with $c_j = \underline{c}$ receives service with the lowest priority with probability one. In turn, any strictly positive fee by a User j with $c_j = \underline{c}$ is dominated by paying a zero fee because the lower fee directly increases User j's utility without increasing her expected wait time. Then, solving (C.12) explicitly and imposing $\phi(\underline{c}) = 0$ yields:

$$\phi(c) = \frac{N-1}{\bar{c} - \underline{c}} \times \frac{c^2 - \underline{c}^2}{2\Lambda} \tag{C.13}$$

for $c \leq c_*$. Note that $\phi(c) = 0$ when $c > c_*$ because, per Definition 1 (i), we subsequently determine c_* such that any User i with $c_i > c_*$ prefers the traditional alternative. Consequently, any User i with $c_i > c_*$ optimally selects a fee $\phi(c_i) = 0$. Explicitly, ϕ is given as follows:

$$\phi(c) = \frac{N-1}{\bar{c}-\underline{c}} \times \frac{c^2-\underline{c}^2}{2\Lambda} \text{ if } c \leq c_* \text{ and } \phi(c) = 0 \text{ otherwise} \tag{C.14}$$

which proves (A).

Establishing (B) - (D)

Definition 1 (ii) and (v) imply:

$$\beta M = B + \mathbb{E}[\sum_i \phi(c_i)] \tag{C.15}$$

Then, invoking symmetry of user types (i.e., c_i are i.i.d) yields:

$$\beta M = B + N \times \mathbb{E}[\phi(c_1)] \tag{C.16}$$

Further, invoking our solution for ϕ from Eqs. (C.14), (C.16) becomes:

$$\beta M = B + N \int_{\underline{c}}^{c_*} \left(\frac{N-1}{\bar{c}-\underline{c}} \times \frac{c^2-\underline{c}^2}{2\Lambda} \right) \times \frac{1}{\bar{c}-\underline{c}} dc \tag{C.17}$$

Evaluating the integral on the right-hand side and dividing by β then establishes (B):

$$M = M(c_*) \equiv \frac{B}{\beta} + \frac{N(N-1)}{6\beta\Lambda} \frac{(c_*-\underline{c}) \cdot (c_*^2 + c_*\underline{c} - 2\underline{c}^2)}{(\bar{c}-\underline{c})^2} \tag{C.18}$$

To establish (C), note that if $c_* \in (\underline{c}, \bar{c})$, then for arbitrarily small $\varepsilon > 0$, Definition 1 (i) and (ii) imply that adopting users (i.e., any User c_i such that $c_i \leq c_*$) find adoption optimal. More formally, the following equation must hold:

$$\max_{f \geq 0} \left(R_1 \cdot (\pi_* N)^\alpha + R_0 - (c_* - \varepsilon) \cdot \mathbb{E}[W(f, \phi(c_{-i}))] - f \right) \geq 0 \tag{C.19}$$

Moreover, Definition 1 (i) and (ii) also imply that non-adopting users (i.e., any User c_i such that $c_i > c_*$) find non-adoption optimal so that the following equation must also hold:

$$\max_{f \geq 0} \left(R_1 \cdot (\pi_* N)^\alpha + R_0 - (c_* + \varepsilon) \cdot \mathbb{E}[W(f, \phi(c_{-i}))] - f \right) < 0 \tag{C.20}$$

Then, taking $\varepsilon \to 0^+$ in both Eqs. (C.19) and (C.20) collectively imply that the marginal user (i.e., any User c_i such that $c_i = c_*$) is indifferent between adoption and non-adoption:

$$\max_{f \geq 0} \left(R_1 \cdot (\pi_* N)^\alpha + R_0 - c_* \cdot \mathbb{E}[W(f, \phi(c_{-i}))] - f \right) = 0 \tag{C.21}$$

In turn, applying Definition 1 (ii) and (iii) which requires that the marginal user pay the optimal fee (i.e., $f_i = \phi(c_*)$ for any User i such that $c_i = c_*$) implies:

$$R_1 \cdot (\pi_* N)^\alpha + R_0 - c_* \cdot \mathbb{E}[W(\phi(c_*), \phi(c_{-i}))] - \phi(c_*) = 0 \tag{C.22}$$

Recall that the marginal user pays the highest fee (i.e., ϕ is increasing over $[\underline{c}, c_*]$ and zero thereafter) so that, with probability one, she does not have to wait for any other users to receive service ahead of her. As a consequence, her wait equals the sum of her individual service time, $\frac{1}{\Lambda}$, and the consensus wait time, $\tau(\Lambda, \Delta(M))$. Then, since $\Psi(\Lambda, \Delta(M)) \equiv \frac{1}{\Lambda} + \tau(\Lambda, \Delta(M))$, Eq. (C.22) becomes:

$$R_1 \cdot (\pi_* N)^\alpha + R_0 - c_* \cdot \Psi(\Lambda, \Delta(M)) - \phi(c_*) = 0 \tag{C.23}$$

and applying Eq. (2) and the previously derived results (A) and (B) to Eq. (C.23) then yields:

$$\begin{aligned} R_1 \cdot \left(\left(\frac{c_* - \underline{c}}{\bar{c}-\underline{c}} \right) \cdot N \right)^\alpha + R_0 = c_* \cdot \Psi(\Lambda, \Delta(M(c_*))) \\ + \frac{N-1}{\bar{c}-\underline{c}} \times \frac{c_*^2 - \underline{c}^2}{2\Lambda} \end{aligned} \tag{C.24}$$

which establishes (C). Note that (C) employs the hypothesis $R_1 \cdot N^\alpha + R_0 < \bar{c} \cdot \Psi(\Lambda, \Delta(M(\bar{c}))) + (N-1) \times \frac{\bar{c}+\underline{c}}{2\Lambda}$, which we have not yet used. This hypothesis will be employed in the last part of this proof to establish existence of c_* and M that satisfy all equilibrium conditions.

Turning to (D), note that Definition 1 (i) implies that, if $c_* = \bar{c}$, then any User i with $c_i = \bar{c}$ must find adoption optimal:

$$\max_{f \geq 0} \left(R_1 \cdot (\pi_* N)^\alpha + R_0 - \bar{c} \cdot \mathbb{E}[W(f, f_{-i})] - f \right) \geq 0 \tag{C.25}$$

Definition 1 (ii) then implies that User i anticipates all other user fees are given by the equilibrium fee function (i.e., $f_{-i} = \phi(c_{-i})$) so that Eq. (C.25) implies:

$$\max_{f \geq 0} \left(R_1 \cdot (\pi_* N)^\alpha + R_0 - \bar{c} \cdot \mathbb{E}[W(f, \phi(c_{-i}))] - f \right) \geq 0 \tag{C.26}$$

In turn, Definition 1 (ii) and (iii) collectively imply that any User i with $c_i = \bar{c}$ selects her fee optimally (i.e., $f_i = \phi(\bar{c})$ when $c_i = \bar{c}$) so that Eq. (C.26) implies:

$$R_1 \cdot (\pi_* N)^\alpha + R_0 - \bar{c} \cdot \mathbb{E}[W(\phi(\bar{c}), \phi(c_{-i}))] - \phi(\bar{c}) \geq 0 \tag{C.27}$$

Recall that ϕ is increasing over $[\underline{c}, c_*]$ and hence over $[\underline{c}, \bar{c}]$ when $c_* = \bar{c}$. In turn, a User i with $c_i = \bar{c}$ receives service first with probability one whenever $c_* = \bar{c}$ and her wait equals $\Psi(\Lambda, \Delta(M))$. Consequently, Eq. (C.27) becomes:

$$R_1 \cdot (\pi_* N)^\alpha + R_0 - \bar{c} \cdot \Psi(\Lambda, \Delta(M)) - \phi(\bar{c}) \geq 0 \tag{C.28}$$

Further, applying Eq. (2) and the previously derived results (A) and (B) to Eq. (C.28) with $c_* = \bar{c}$ then yields:

$$R_1 \cdot N^\alpha + R_0 \geq \bar{c} \cdot \Psi(\Lambda, \Delta(M(\bar{c}))) + (N-1) \times \frac{\bar{c}+\underline{c}}{2\Lambda} \tag{C.29}$$

which is the hypothesis for (D). Note that (D) asserts that this hypothesis implies a full adoption equilibrium (i.e., $c_* = \bar{c}$). Thus far, we have shown only that this hypothesis is the condition for adoption to be optimal for any User i with $c_i = \bar{c}$ in a full adoption equilibrium (i.e., when $c_* = \bar{c}$). To complete this portion of the proof, we must demonstrate that Eq. (C.29) implies also that adoption is optimal for any User i such that $c_i < \bar{c}$. As we demonstrate subsequently, that fact follows from the user utility of an adopting user decreasing in c_i. More formally, we let U denote the user utility of any adopting User i (i.e., $c \le c_*$) in any equilibrium with cut-off c_* so that U is given as follows:

$$U(c, c_*) \equiv \max_{f \ge 0} \left(R_1 \cdot \left(\left(\frac{c_* - \underline{c}}{\bar{c} - \underline{c}} \right) \cdot N \right)^{\alpha} + R_0 \right.$$
$$\left. - c \cdot \mathbb{E}[W(f, \phi(c_{-i}))] - f \right) \tag{C.30}$$

and we let $\tilde{U}$ denote the utility of any adopting User i (i.e., $c \le c_*$) when she selects fee f so that $\tilde{U}$ is given as follows:

$$\tilde{U}(c, f, c_*) \equiv R_1 \cdot \left(\left(\frac{c_* - \underline{c}}{\bar{c} - \underline{c}} \right) \cdot N \right)^{\alpha}$$
$$+ R_0 - c \cdot \mathbb{E}[W(f, \phi(c_{-i}))] - f \tag{C.31}$$

Definitions 1 (ii) and (iii) require that User i's fee is set optimally (i.e., $f_i = \phi(c_i)$) so that the following equation holds for any $c_i \le c_*$ in any equilibrium:

$$U(c_i, c_*) = \tilde{U}(c_i, \phi(c_i), c_*) \tag{C.32}$$

Then, differentiating with respect to c yields:

$$\frac{\partial U(c_i, c_*)}{\partial c} = \frac{\partial \tilde{U}(c_i, \phi(c_i), c_*)}{\partial c} + \frac{\partial \tilde{U}(c_i, \phi(c_i), c_*)}{\partial f} \times \frac{d\phi(c_i)}{dc} \tag{C.33}$$

Note that the first-order condition in the derivation of (A) implies that $\frac{\partial \tilde{U}(c_i, \phi(c_i), c_*)}{\partial f} = 0$ so that direct computation from Eqs. (C.31) and (C.33) yield:

$$\frac{\partial U(c_i, c_*)}{\partial c} = \frac{\partial \tilde{U}(c_i, \phi(c_i), c_*)}{\partial c} = -\mathbb{E}[W(\phi(c_i), \phi(c_{-i}))] < 0 \tag{C.34}$$

Recall that Eq. (C.28) corresponds to the condition that any User i with $c_i = \bar{c}$ finds adoption optimal in a full adoption equilibrium (i.e., when $c_* = \bar{c}$). More formally, Eq. (C.28) is equivalent to $U(\bar{c}, \bar{c}) \ge 0$ so that Eq. (C.34) implies that adoption is optimal for all Users (i.e., $U(c_i, \bar{c}) \ge 0$ for all $c_i \le \bar{c}$), which thus establishes (D).

Existence of c_* and M

As just shown, when Eq. (C.28) holds, then a full adoption equilibrium arises. In such an equilibrium, solutions for c_* and M are given explicitly by:

$$c_* = \bar{c}, \qquad M = M(\bar{c}) \tag{C.35}$$

When Eq. (C.28) does not hold, then a full adoption equilibrium cannot arise since Eq. (C.28) is the condition for a User i with $c_i = \bar{c}$ to find adoption optimal and therefore is a necessary condition for a full adoption equilibrium. Consequently, in such a case, only an equilibrium such that $c_* \in (\underline{c}, \bar{c})$ can arise. We subsequently demonstrate the existence of such an equilibrium. More formally, we demonstrate existence of c_* and M such that (B) and (C) both hold. Note that (A) holds for any given c_* and (D) is not relevant because it applies only when Eq. (C.28) holds. In turn, existence of c_* and M satisfying (B) and (C) suffices to establish existence of an equilibrium for model parameters such that Eq. (C.28) does not hold.

Note that Eq. (C.28) corresponds to a User i such that $c_i = \bar{c}$ finding not adopting optimal whenever $c_* = \bar{c}$. More formally, in this case, the following equation must hold:

$$U(\bar{c}, \bar{c}) < 0 \tag{C.36}$$

Recall that we impose $R_0 > \underline{c} \cdot (\frac{1}{\Lambda} + \tau(\Lambda, \Delta(\frac{B}{\beta})))$, which ensures that adopting is optimal whenever $c_* = \underline{c}$ (i.e., non-adoption for all users is not an equilibrium). Explicitly, $R_0 > \underline{c} \cdot (\frac{1}{\Lambda} + \tau(\Lambda, \Delta(\frac{B}{\beta})))$ is equivalent to:

$$U(\underline{c}, \underline{c}) > 0 \tag{C.37}$$

Then, Eqs. (C.36)-(C.37), and continuity of $U^*(c) \equiv U(c, c)$ implies the existence of $\tilde{c}_* \in (\underline{c}, \bar{c})$ such that $U^*(\tilde{c}_*) = 0$. Note that $U^*(\tilde{c}_*) = 0$ is equivalent to (C) if Eq. (C.28) does not hold. In turn, the equilibrium c_* and M are given explicitly as follows:

$$c_* = \tilde{c}_*, \qquad M = M(\tilde{c}_*) \tag{C.38}$$

where the latter equation satisfies (B) and thereby completes the proof. □

C2. Preliminary lemmas

Lemma 12. Interior Adoption Rate For Large N

Suppose that the transaction rate, $\Lambda > 0$, is fixed. Then, there exists $\underline{N} > 0$ such that for all $N > \underline{N}$, we have the following:

$$R_1 \cdot N^{\alpha} + R_0 < \bar{c} \cdot \Psi(\Lambda, \Delta(M(\bar{c}))) + (N - 1) \times \frac{\bar{c} + \underline{c}}{2\Lambda}$$

where $M(c)$ is defined explicitly in Proposition 1.

Proof. $\alpha \in (0, 1)$ implies that $\lim_{N \to \infty} \frac{N-1}{N^{\alpha}} = \infty$ which further implies:

$$\lim_{N \to \infty} \left(R_1 \cdot N^{\alpha} + R_0 - (N - 1) \times \frac{\bar{c} + \underline{c}}{2\Lambda} \right) = -\infty \tag{C.39}$$

In turn, that implies that there exists $\underline{N}$ such that for all $N > \underline{N}$, we have the following:

$$R_1 \cdot N^{\alpha} + R_0 < (N - 1) \times \frac{\bar{c} + \underline{c}}{2\Lambda} \tag{C.40}$$

and since $\bar{c} \cdot \Psi(\Lambda, M(\bar{c})) \ge 0$, we also have the following for $N > \underline{N}$:

$$R_1 \cdot N^{\alpha} + R_0 < \bar{c} \cdot \Psi(\Lambda, \Delta(M(\bar{c}))) + (N - 1) \times \frac{\bar{c} + \underline{c}}{2\Lambda} \tag{C.41}$$

which completes the proof. □

Lemma 13. Interior Adoption Rate For Large N And Variable Transaction Rate, Λ_N

Suppose that the transaction rate, $\Lambda_N > 0$, is a function of transaction demand, N. Then, there exists $\underline{N} > 0$ such that for all $N > \underline{N}$, we have the following:

$$R_1 \cdot N^{\alpha} + R_0 < \bar{c} \cdot \Psi(\Lambda_N, \Delta(M(\bar{c}))) + (N - 1) \times \frac{\bar{c} + \underline{c}}{2\Lambda_N}$$

where $M(c)$ is define explicitly in Proposition 1.

Proof. We prove this result by contradiction. In particular, if there did not exist an $\underline{N}$ as described in the statement of this lemma, then there must be infinitely many values of N such that:

$$R_1 \cdot N^{\alpha} + R_0 \geq \bar{c} \cdot \Psi(\Lambda_N, \Delta(M(\bar{c}))) + (N-1) \times \frac{\bar{c}+\underline{c}}{2\Lambda_N} \tag{C.42}$$

and we demonstrate that this is not possible.

Note that if there existed infinitely many N such that Eq. (C.42) held for all those N, then we could form a subsequence indexed by N_k such that:

$$R_1 \cdot N_k^{\alpha} + R_0 \geq \bar{c} \cdot \Psi(\Lambda_{N_k}, \Delta(M(\bar{c}))) + (N_k-1) \times \frac{\bar{c}+\underline{c}}{2\Lambda_{N_k}} \tag{C.43}$$

for all k and $\lim_{k\to\infty} N_k = \infty$. On that sub-sequence, either $\liminf_{k\to\infty} \frac{N_k^{1-\alpha}}{\Lambda_{N_k}} = \infty$ or $\liminf_{k\to\infty} \frac{N_k^{1-\alpha}}{\Lambda_{N_k}} < \infty$. We subsequently consider each case and demonstrate that each implies a contradiction, thereby establishing the lemma.

Case 1: $\liminf_{k\to\infty} \frac{N_k^{1-\alpha}}{\Lambda_{N_k}} = \infty$

Equation (C.43) implies:

$$R_1 \cdot N_k^{\alpha} + R_0 \geq (N_k - 1) \times \frac{\bar{c}+\underline{c}}{2\Lambda_{N_k}} \tag{C.44}$$

Equation (C.44) can be re-written as:

$$R_1 \cdot N_k^{\alpha} + R_0 \geq \frac{N_k - 1}{N_k} \times N_k \times \frac{\bar{c}+\underline{c}}{2\Lambda_{N_k}} \tag{C.45}$$

Then, dividing each side of Eq. (C.45) by N_k^{α} yields:

$$R_1 + \frac{R_0}{N_k^{\alpha}} \geq \frac{N_k - 1}{N_k} \times N_k^{1-\alpha} \times \frac{\bar{c}+\underline{c}}{2\Lambda_{N_k}} \tag{C.46}$$

Note that $\inf_k \left(\frac{N_k-1}{N_k} \times N_k^{1-\alpha} \times \frac{\bar{c}+\underline{c}}{2\Lambda_{N_k}} \right) \geq \frac{\bar{c}+\underline{c}}{2} \times \inf_k \frac{N_k-1}{N_k} \times \inf_k \frac{N_k^{1-\alpha}}{\Lambda_{N_k}} \geq \frac{\bar{c}+\underline{c}}{4} \times \inf_k \frac{N_k^{1-\alpha}}{\Lambda_{N_k}}$ where the last inequality follows because $N_k \geq 2$ for all k implies $\frac{N_k-1}{N_k} \geq \frac{1}{2}$ for all k. As a consequence, Eq. (C.46) implies:

$$R_1 + \frac{R_0}{N_k^{\alpha}} \geq \frac{\bar{c}+\underline{c}}{4} \times \inf_k \frac{N_k^{1-\alpha}}{\Lambda_{N_k}} \tag{C.47}$$

Taking limits on both sides as $k \to \infty$ implies $R_1 = \infty$, which yields the desired contradiction since R_1 is a finite model parameter.

Case 2: $\liminf_{k\to\infty} \frac{N_k^{1-\alpha}}{\Lambda_{N_k}} < \infty$

Note that there must exist a further sub-sequence of the sub-sequence indexed by N_{k_l} such that the further sub-sequence converges to $\liminf_{k\to\infty} \frac{N_k^{1-\alpha}}{\Lambda_{N_k}}$. Denoting the further sub-sequence by index N_{k_l}, Eq. (C.43) implies:

$$R_1 \cdot N_{k_l}^{\alpha} + R_0 \geq \bar{c} \cdot \Psi(\Lambda_{N_{k_l}}, \Delta(M(\bar{c}))) \tag{C.48}$$

for all $l \in \mathbb{N}$ with $\lim_{l\to\infty} N_{k_l} = \infty$.

Proposition 1 (B) implies that $M(\bar{c}) \geq \frac{B}{\beta}$. Moreover, Lemma 6 and $p(\Lambda, \Delta) = 1 - e^{-\Lambda\Delta}$ increasing in Δ imply that $\Psi(\Lambda, \Delta)$ increases in Δ so that $\Psi(\Lambda_{N_{k_l}}, \Delta(M(\bar{c}))) \geq \Psi(\Lambda_{N_{k_l}}, \Delta(\frac{B}{\beta}))$. In turn, applying those facts to Eq. (C.48) yields:

$$R_1 \cdot N_{k_l}^{\alpha} + R_0 \geq \bar{c} \cdot \Psi(\Lambda_{N_{k_l}}, \Delta(\frac{B}{\beta})) \tag{C.49}$$

Lemma 8 implies $\Psi(\Lambda_{N_{k_l}}, \Delta(\frac{B}{\beta})) \geq \frac{e^{\Lambda_{N_{k_l}}\Delta(\frac{B}{\beta})}-1}{\Lambda_{N_{k_l}}}$ so that Eq. (C.49) implies:

$$R_1 \cdot N_{k_l}^{\alpha} + R_0 \geq \bar{c} \cdot \frac{e^{\Lambda_{N_{k_l}}\Delta(\frac{B}{\beta})} - 1}{\Lambda_{N_{k_l}}} \tag{C.50}$$

Note that $e^x - 1 = \sum_{n=1}^{\infty} \frac{x^n}{n!} \geq \frac{x^{\nu}}{\nu!}$ when $x \geq 0$ where $\nu \equiv \lceil \frac{\alpha}{1-\alpha} + 2 \rceil$. Then, $\frac{e^{\Lambda_{N_k}\Delta(\frac{B}{\beta})}-1}{\Lambda_{N_k}} \geq \frac{1}{\nu!} \cdot \frac{(\Lambda_{N_k}\Delta(\frac{B}{\beta}))^{\nu}}{\Lambda_{N_k}} \geq \frac{1}{\nu!} \cdot \Lambda_{N_k}^{\nu-1} \cdot \Delta(\frac{B}{\beta})^{\nu}$ so that Eq. (C.50) implies:

$$R_1 \cdot N_{k_l}^{\alpha} + R_0 \geq \frac{\bar{c}}{\nu!} \cdot \Lambda_{N_{k_l}}^{\nu-1} \cdot \Delta(\frac{B}{\beta})^{\nu} \tag{C.51}$$

Moreover, since $\Lambda_{N_k}^{\nu-1} = (\frac{\Lambda_{N_k}}{N_k^{1-\alpha}})^{(\nu-1)} \cdot N_k^{(1-\alpha)\cdot(\nu-1)}$, Eq. (C.51) can be re-written as:

$$R_1 \cdot N_{k_l}^{\alpha} + R_0 \geq \frac{\bar{c}}{\nu!} \cdot (\frac{\Lambda_{N_{k_l}}}{N_{k_l}^{1-\alpha}})^{\nu-1} \cdot N_{k_l}^{(1-\alpha)\cdot(\nu-1)} \cdot \Delta(\frac{B}{\beta})^{\nu} \tag{C.52}$$

In turn, dividing both sides by $N_{k_l}^{\alpha}$ yields:

$$R_1 + \frac{R_0}{N_{k_l}^{\alpha}} \geq \frac{\bar{c}}{\nu!} \cdot (\frac{\Lambda_{N_{k_l}}}{N_{k_l}^{1-\alpha}})^{\nu-1} \cdot N_{k_l}^{(1-\alpha)\cdot(\nu-1)-\alpha} \cdot \Delta(\frac{B}{\beta})^{\nu} \tag{C.53}$$

$\lim_{l\to\infty} \frac{\Lambda_{N_{k_l}}}{N_{k_l}^{1-\alpha}} = \frac{1}{\lim_{l\to\infty} \frac{N_{k_l}^{1-\alpha}}{\Lambda_{N_{k_l}}}} = \frac{1}{\liminf_{k\to\infty} \frac{N_k^{1-\alpha}}{\Lambda_{N_k}}} > 0$ where the second equality follows from the further sub-sequence being constructed to converge to $\liminf_{k\to\infty} \frac{N_k^{1-\alpha}}{\Lambda_{N_k}}$, and the strict inequality follows from $\liminf_{k\to\infty} \frac{N_k^{1-\alpha}}{\Lambda_{N_k}} < \infty$. Moreover, recall that $\nu \equiv \lceil \frac{\alpha}{1-\alpha} + 2 \rceil$ so that $(1-\alpha)\cdot(\nu-1) \geq (1-\alpha)\cdot(\frac{\alpha}{1-\alpha}+1) = 1$. In turn, $(1-\alpha)\cdot(\nu-1)-\alpha \geq 1-\alpha > 0$ so that $\lim_{l\to\infty} N_{k_l}^{(1-\alpha)\cdot(\nu-1)-\alpha} = \infty$ because $\lim_{l\to\infty} N_{k_l} = \infty$. Then, since $\lim_{l\to\infty} \frac{\Lambda_{N_{k_l}}}{N_{k_l}^{1-\alpha}} > 0$ and $\lim_{l\to\infty} N_{k_l}^{(1-\alpha)\cdot(\nu-1)-\alpha} = \infty$, taking $l \to \infty$ on both sides of Eq. (C.53) implies $R_1 = \infty$, which generates the desired contradiction. $R_1 = \infty$ is a contradiction because R_1 is a finite parameter of our model. □

Lemma 14. Bounded Adoption Eventually Implies Uniformly Bounded Adoption

If the adoption level, $\pi_* N$, is bounded as $N \to \infty$ (i.e., $\limsup_{N\to\infty} \pi_* N < \infty$), then the adoption level is bounded uniformly for all N (i.e., $\sup_{N\in\mathbb{N}} \pi_* N < \infty$).

Proof. Let $L \equiv \limsup_{N\to\infty} \pi_* N < \infty$. Then, by definition, there exists $N_{\varepsilon} < \infty$ such that $\sup_{N\in\mathbb{N}:N\geq N_{\varepsilon}} \pi_* N \leq L + \varepsilon < \infty$

where $\varepsilon > 0$ and $\varepsilon < \infty$. Additionally, note that $\pi_* \in [0,1]$ so that $\sup_{N \in \mathbb{N}: N \le N_\varepsilon} \pi_* N \le N_\varepsilon$. Thus, $\sup_{N \in \mathbb{N}} \pi_* N \le \max\{ \sup_{N \in \mathbb{N}: N \le N_\varepsilon} \pi_* N, \sup_{N \in \mathbb{N}: N \ge N_\varepsilon} \pi_* N\} \le \max\{N_\varepsilon, L + \varepsilon\} < \infty$, thereby completing the proof. □

C3. Proofs for Section 4

Proof of Proposition 6.. Lemma 14 yields that $\limsup_{N \to \infty} \pi_* N < \infty \Rightarrow \sup_{N \in \mathbb{N}} \pi_* N < \infty$, so it suffices to show $\limsup_{N \to \infty} \pi_* N < \infty$. We establish that result by contradiction. In particular, we assume $\limsup_{N \to \infty} \pi_* N = \infty$ and demonstrate that this yields a contradiction, thereby establishing $\limsup_{N \to \infty} \pi_* N < \infty$ and, via Lemma 14, also $\sup_{N \in \mathbb{N}} \pi_* N < \infty$.

Lemma 12 and Proposition 1 (C) collectively imply that there exists an $\underline{N}$ such that for all $N > \underline{N}$, the following equation holds:

$$R_1 \cdot \left(\frac{c_* - \underline{c}}{\bar{c} - \underline{c}} \right)^\alpha \cdot N^\alpha + R_0 = c_* \Psi(\Lambda, \Delta(M(c_*))) + \frac{N-1}{\bar{c} - \underline{c}} \times \frac{c_*^2 - \underline{c}^2}{2\Lambda} \tag{C.54}$$

which implies:

$$R_1 \cdot \left(\frac{c_* - \underline{c}}{\bar{c} - \underline{c}} \right)^\alpha \cdot N^\alpha + R_0 \ge \frac{N-1}{\bar{c} - \underline{c}} \times \frac{c_*^2 - \underline{c}^2}{2\Lambda} \tag{C.55}$$

for $N > \underline{N}$. Then, using $\pi_* = \frac{c_* - \underline{c}}{\bar{c} - \underline{c}}$, implies:

$$R_1 \cdot (\pi_* N)^\alpha + R_0 \ge \frac{N-1}{N} \times (\pi_* N) \times \frac{c_* + \underline{c}}{2\Lambda} \tag{C.56}$$

for all $N > \underline{N}$. Further, using $c_* \ge \underline{c}$ yields:

$$R_1 \cdot (\pi_* N)^\alpha + R_0 \ge \frac{N-1}{N} \times (\pi_* N) \times \frac{\underline{c}}{\Lambda} \tag{C.57}$$

Then, dividing through by $(\pi_* N)^\alpha$ and isolating $(\pi_* N)^{1-\alpha}$ yields:

$$(\pi_* N)^{1-\alpha} \le \left(\frac{N}{N-1} \right) \times \left(\frac{\Lambda}{\underline{c}} \right) \cdot \left(R_1 + \frac{R_0}{(\pi_* N)^\alpha} \right) \tag{C.58}$$

for all $N > \underline{N}$. Note that there must exist a sub-sequence starting after index $N = \underline{N}$ along which $\pi_* N$ converges to $\limsup_{N \to \infty} \pi_* N = \infty$. As a consequence, indexing such a sub-sequence by N_k yields:

$$(\pi_* N_k)^{1-\alpha} \le \left(\frac{N_k}{N_k - 1} \right) \times \left(\frac{\Lambda}{\underline{c}} \right) \cdot \left(R_1 + \frac{R_0}{(\pi_* N_k)^\alpha} \right) \tag{C.59}$$

for all k with $\lim_{k \to \infty} N_k = \infty$ and $\lim_{k \to \infty} \pi_* N_k = \infty$. In turn, taking $k \to \infty$ in Eq. (C.59) yields:

$$\infty = \lim_{k \to \infty} (\pi_* N_k)^{1-\alpha} \le \lim_{k \to \infty} \left\{ \left(\frac{N_k}{N_k - 1} \right) \times \left(\frac{\Lambda}{\underline{c}} \right) \times \left(R_1 + \frac{R_0}{(\pi_* N_k)^\alpha} \right) \right\} \le \frac{\Lambda \cdot R_1}{\underline{c}} \tag{C.60}$$

but Λ, R_1 and $\underline{c}$ are all finite model parameters, implying that that $\frac{\Lambda R_1}{\underline{c}} < \infty$ so that Eq. (C.60) delivers a contradiction and completes the proof. □

Proof of Proposition 7. Lemma 14 yields that $\limsup_{N \to \infty} \pi_* N < \infty \Rightarrow \sup_{N \in \mathbb{N}} \pi_* N < \infty$, so it suffices to show $\limsup_{N \to \infty} \pi_* N < \infty$. We establish that result by contradiction. In particular, we assume $\limsup_{N \to \infty} \pi_* N = \infty$ and demonstrate that this yields a contradiction, thereby establishing $\limsup_{N \to \infty} \pi_* N < \infty$ and, via Lemma 14, also $\sup_{N \in \mathbb{N}} \pi_* N < \infty$.

Lemma 13 and Proposition 1 (C) collectively imply that there exists an $\underline{N}$ such that for all $N > \underline{N}$, the following equation holds:

$$R_1 \cdot \left(\frac{c_* - \underline{c}}{\bar{c} - \underline{c}} \right)^\alpha \cdot N^\alpha + R_0 = c_* \Psi(\Lambda_N, \Delta(M(c_*))) + \frac{N-1}{\bar{c} - \underline{c}} \times \frac{c_*^2 - \underline{c}^2}{2\Lambda_N} \tag{C.61}$$

Note that $\frac{N-1}{\bar{c} - \underline{c}} \times (c_*^2 - \underline{c}^2) = \frac{N-1}{N} \times \frac{N}{\bar{c} - \underline{c}} \times (c_*^2 - \underline{c}^2) = \frac{N-1}{N} \times N \times \frac{c_* - \underline{c}}{\bar{c} - \underline{c}} \times (c_* + \underline{c}) = \frac{N-1}{N} \times (\pi_* N) \times (c_* + \underline{c})$. Then, invoking $\pi_* = \frac{c_* - \underline{c}}{\bar{c} - \underline{c}}$ in Eq. (C.61) implies:

$$R_1 \cdot (\pi_* N)^\alpha + R_0 = c_* \Psi(\Lambda_N, \Delta(M(c_*))) + \frac{N-1}{N} \times (\pi_* N) \times \frac{c_* + \underline{c}}{2\Lambda_N} \tag{C.62}$$

for all $N > \underline{N}$. Moreover, since $\limsup_{N \to \infty} \pi_* N = \infty$, there exists a sub-sequence indexed by N_k such that:

$$R_1 \cdot (\pi_* N_k)^\alpha + R_0 = c_* \Psi(\Lambda_{N_k}, \Delta(M(c_*))) + \frac{N_k - 1}{N_k} \times (\pi_* N_k) \times \frac{c_* + \underline{c}}{2\Lambda_{N_k}} \tag{C.63}$$

for all k with $\lim_{k \to \infty} N_k = \infty$ and $\lim_{k \to \infty} \pi_* N_k = \infty$. On this sub-sequence, either $\liminf_{k \to \infty} \frac{(\pi_* N_k)^{1-\alpha}}{\Lambda_{N_k}} = \infty$ or $\liminf_{k \to \infty} \frac{(\pi_* N_k)^{1-\alpha}}{\Lambda_{N_k}} < \infty$. We subsequently consider each case separately.

Case 1: $\liminf_{k \to \infty} \frac{(\pi_* N_k)^{1-\alpha}}{\Lambda_{N_k}} = \infty$

Equation (C.63) implies:

$$R_1 \cdot (\pi_* N_k)^\alpha + R_0 \ge \frac{N_k - 1}{N_k} \times (\pi_* N_k) \times \frac{c_* + \underline{c}}{2\Lambda_{N_k}} \tag{C.64}$$

Note that $c_* \ge \underline{c}$ so that Eq. (C.64) implies:

$$R_1 \cdot (\pi_* N_k)^\alpha + R_0 \ge \frac{N_k - 1}{N_k} \times (\pi_* N_k) \times \frac{\underline{c}}{\Lambda_{N_k}} \tag{C.65}$$

Dividing each side in Eq. (C.66) by $(\pi_* N)^\alpha$ then yields:

$$R_1 + \frac{R_0}{(\pi_* N_k)^\alpha} \ge \frac{N_k - 1}{N_k} \times (\pi_* N_k)^{1-\alpha} \times \frac{\underline{c}}{\Lambda_{N_k}} \tag{C.66}$$

Note that $\frac{N_k - 1}{N_k} \times (\pi_* N_k)^{1-\alpha} \times \frac{\underline{c}}{\Lambda_{N_k}} \ge \inf_k \left(\frac{N_k - 1}{N_k} \times (\pi_* N_k)^{1-\alpha} \times \frac{\underline{c}}{\Lambda_{N_k}} \right) \ge \inf_k \frac{N_k - 1}{N_k} \times \underline{c} \times \inf_k \frac{(\pi_* N_k)^{1-\alpha}}{\Lambda_{N_k}} \ge \frac{\underline{c}}{2} \times \inf_k \frac{(\pi_* N_k)^{1-\alpha}}{\Lambda_{N_k}}$ where the last inequality uses $N_k \ge 2$ for all k. Note also that $\frac{R_0}{\inf_k (\pi_* N_k)^\alpha} \ge \frac{R_0}{(\pi_* N_k)^\alpha}$. In turn, Eq. (C.66) implies:

$$R_1 + \frac{R_0}{\inf_k (\pi_* N_k)^\alpha} \ge \frac{\underline{c}}{2} \times \inf_k \frac{(\pi_* N)^{1-\alpha}}{\Lambda_{N_k}} \tag{C.67}$$

Then, taking limits as $k \to \infty$ implies $R_1 = \infty$, which delivers the desired contradiction since R_1 is a finite parameter of our model.

Case 2: $\liminf_{k\to\infty} \frac{(\pi_* N_k)^{1-\alpha}}{\Lambda_{N_k}} < \infty$

Equation (C.63) implies:

$$R_1 \cdot (\pi_* N_k)^{\alpha} + R_0 \geq c_* \Psi(\Lambda_{N_k}, \Delta(M(c_*))) \tag{C.68}$$

Proposition 1 (B) implies that $M(c_*) \geq \frac{B}{\beta}$ for any c_*. Moreover, Lemma 6 and $p(\Lambda, \Delta) = 1 - e^{-\Lambda\Delta}$ increasing in Δ imply that $\Psi(\Lambda, \Delta)$ increases in Δ so that $\Psi(\Lambda_{N_k}, \Delta(M(c_*))) \geq \Psi(\Lambda_{N_k}, \Delta(\frac{B}{\beta}))$. In turn, applying those facts and $c_* \geq \underline{c}$ to Eq. (C.68) yields:

$$R_1 \cdot (\pi_* N_k)^{\alpha} + R_0 \geq \underline{c} \cdot \Psi(\Lambda_{N_k}, \Delta(\frac{B}{\beta})) \tag{C.69}$$

Lemma 8 implies $\Psi(\Lambda_{N_k}, \Delta(\frac{B}{\beta})) \geq \frac{e^{\Lambda_{N_k}\Delta(\frac{B}{\beta})}-1}{\Lambda_{N_k}}$ so that Eq. (C.69) implies:

$$R_1 \cdot (\pi_* N_k)^{\alpha} + R_0 \geq \underline{c} \cdot \frac{e^{\Lambda_{N_k}\Delta(\frac{B}{\beta})} - 1}{\Lambda_{N_k}} \tag{C.70}$$

Note that $e^x - 1 = \sum_{n=1}^{\infty} \frac{x^n}{n!} \geq \frac{x^{\nu}}{\nu!}$ when $x \geq 0$ where $\nu \equiv \lceil \frac{\alpha}{1-\alpha} + 2 \rceil$. Then, $\frac{e^{\Lambda_{N_k}\Delta(\frac{B}{\beta})}-1}{\Lambda_{N_k}} \geq \frac{1}{\nu!} \cdot \frac{(\Lambda_{N_k}\Delta(\frac{B}{\beta}))^{\nu}}{\Lambda_{N_k}} \geq \frac{1}{\nu!} \cdot \Lambda_{N_k}^{\nu-1} \cdot \Delta(\frac{B}{\beta})^{\nu}$ so that Eq. (C.70) implies:

$$R_1 \cdot (\pi_* N_k)^{\alpha} + R_0 \geq \frac{\underline{c}}{\nu!} \cdot \Lambda_{N_k}^{\nu-1} \cdot \Delta(\frac{B}{\beta})^{\nu} \tag{C.71}$$

Moreover, since $\Lambda_{N_k}^{\nu-1} = (\frac{\Lambda_{N_k}}{(\pi_* N_k)^{1-\alpha}})^{(\nu-1)} \cdot (\pi_* N_k)^{(1-\alpha)\cdot(\nu-1)}$, Eq. (C.71) can be re-written as:

$$R_1 \cdot (\pi_* N_k)^{\alpha} + R_0 \geq \frac{\underline{c}}{\nu!} \cdot (\frac{\Lambda_{N_k}}{(\pi_* N_k)^{1-\alpha}})^{(\nu-1)} \cdot (\pi_* N_k)^{(1-\alpha)\cdot(\nu-1)} \cdot \Delta(\frac{B}{\beta})^{\nu} \tag{C.72}$$

Dividing through by $(\pi_* N_k)^{\alpha}$ then yields:

$$R_1 + \frac{R_0}{(\pi_* N_k)^{\alpha}} \geq \frac{\underline{c}}{\nu!} \cdot (\frac{\Lambda_{N_k}}{(\pi_* N_k)^{1-\alpha}})^{(\nu-1)} \cdot (\pi_* N_k)^{(1-\alpha)\cdot(\nu-1)-\alpha} \cdot \Delta(\frac{B}{\beta})^{\nu} \tag{C.73}$$

Note that there exists a further sub-sequence that converges to $\liminf_{k\to\infty} \frac{(\pi_* N_k)^{1-\alpha}}{\Lambda_{N_k}}$. Explicitly, indexing that further sub-sequence by N_{k_l}, we have that $\lim_{l\to\infty} \frac{(\pi_* N_{k_l})^{1-\alpha}}{\Lambda_{N_{k_l}}} = \liminf_{k\to\infty} \frac{(\pi_* N_k)^{1-\alpha}}{\Lambda_{N_k}}$ due to the construction of the further sub-sequence. Note also that $\lim_{l\to\infty} N_{k_l} = \infty$ and $\lim_{l\to\infty} \pi_* N_{k_l} = \infty$ because $\lim_{k\to\infty} N_k = \infty$ and $\lim_{k\to\infty} \pi_* N_k = \infty$. Since Eq. (C.73) holds for all k, it also holds for all k_l. More explicitly:

$$R_1 + \frac{R_0}{(\pi_* N_{k_l})^{\alpha}} \geq \frac{\underline{c}}{\nu!} \cdot (\frac{\Lambda_{N_{k_l}}}{(\pi_* N_{k_l})^{1-\alpha}})^{(\nu-1)} \cdot (\pi_* N_{k_l})^{(1-\alpha)\cdot(\nu-1)-\alpha} \cdot \Delta(\frac{B}{\beta})^{\nu} \tag{C.74}$$

$$\lim_{l\to\infty} \frac{\Lambda_{N_{k_l}}}{(\pi_* N_{k_l})^{1-\alpha}} = \frac{1}{\lim_{l\to\infty} \frac{(\pi_* N_{k_l})^{1-\alpha}}{\Lambda_{N_{k_l}}}} = \frac{1}{\liminf_{k\to\infty} \frac{(\pi_* N_k)^{1-\alpha}}{\Lambda_{N_k}}} > 0$$

where the second equality follows from the further sub-sequence being constructed to converge to $\liminf_{k\to\infty} \frac{(\pi_* N_k)^{1-\alpha}}{\Lambda_{N_k}}$, and the strict inequality follows from $\liminf_{k\to\infty} \frac{(\pi_* N_k)^{1-\alpha}}{\Lambda_{N_k}} < \infty$. Moreover, recall that $\nu \equiv \lceil \frac{\alpha}{1-\alpha} + 2 \rceil$ so that $(1-\alpha) \cdot (\nu - 1) \geq (1-\alpha) \cdot (\frac{\alpha}{1-\alpha} + 1) = 1$. In turn, $(1-\alpha) \cdot (\nu - 1) - \alpha \geq 1 - \alpha > 0$ so that $\lim_{l\to\infty} (\pi_* N_{k_l})^{(1-\alpha)\cdot(\nu-1)-\alpha} = \infty$ because $\lim_{l\to\infty} \pi_* N_{k_l} = \infty$. Then, since $\lim_{l\to\infty} \frac{\Lambda_{N_{k_l}}}{(\pi_* N_{k_l})^{1-\alpha}} > 0$ and $\lim_{l\to\infty} (\pi_* N_{k_l})^{(1-\alpha)\cdot(\nu-1)-\alpha} = \infty$, taking $l \to \infty$ on both sides of Eq. (C.74) implies $R_1 = \infty$, which generates the desired contradiction. $R_1 = \infty$ is a contradiction because R_1 is a finite parameter of our model. □

Proof of Proposition 8.. As per the hypothesis of the result, we restrict only the transaction rate, Λ, and the network delay function, $\Delta(M)$, in establishing this result. Our result is invariant to any given set of preference parameters in our model.

Explicitly, we require that the transaction rate Λ corresponds to 150 million transactions per day. Moreover, we require that the network delay function, $\Delta(M)$, be such that $\Delta(M) \geq \underline{\Delta}$, whereas $\underline{\Delta}$ is given by empirical estimates in Croman et al. (2016).

It is useful to convert to seconds so the transaction rate, Λ, is given as follows:

$$\Lambda = \frac{150 \times 10^6 \text{ transactions}}{\text{day}} \times \frac{1 \text{ day}}{24 \times 60 \times 60 \text{ seconds}} = 1736 \frac{\text{transactions}}{\text{second}} \tag{C.75}$$

where we round down to the nearest integer. Croman et al. (2016) find that a 1 MB block possesses a median propagation time of 15.7 s. Our network delay function corresponds to the mean propagation time for a single transaction. Thus, assuming that the mean exceeds the median and that a 1 MB block has 2000 transactions, the lower bound for network delay, $\underline{\Delta}$, can itself be bounded below as follows:

$$\underline{\Delta} \geq \frac{15.7 \text{ seconds}}{\text{block}} \times \frac{1 \text{ block}}{2000 \text{ transactions}} \tag{C.76}$$

Note that the network delay data in Croman et al. (2016) is right-skewed, so our assumption regarding the mean exceeding the median is consistent with their data. Moreover, assuming 2000 transactions per block is also consistent with the publicly available data on Bitcoin and is used in Huberman et al. (2021).

Turning to Proposition 8 (A), Eq. (5) implies:

$$p \equiv \mathbb{P}(Fork) \geq 1 - e^{-\Lambda\underline{\Delta}} > 0.99 \tag{C.77}$$

which establishes the first part of Proposition 8 (A). For the second part of Proposition 8 (A), note that Lemma 1 implies that the blockchain is in a fork with probability $1 - (1-p)^b$, where p is the fork probability given by Eq. (C.77), and b is the number of blocks on which the network must agree to regain consensus. Note that $b \geq 1$

by definition so that $1-(1-p)^b \geq 1-(1-p)^1 = p > 0.99$ thereby completing the proof of Proposition 8 (A).

Turning to Proposition 8 (B), recall that the expected wait time for any User i is bounded below by the consensus wait time, and the consensus wait time is identical across users. More explicitly, the following equation holds:

$$\mathbb{E}[W(f_i, f_{-i})] \geq \tau(\Lambda, \Delta(M)) \tag{C.78}$$

Then, since the consensus wait time increases in network delay (see Lemma 6), $\Delta(M) \geq \underline{\Delta}$ applied to Eq. (C.78) yields:

$$\mathbb{E}[W(f_i, f_{-i})] \geq \tau(\Lambda, \underline{\Delta}) \tag{C.79}$$

In turn, computing τ directly yields (see Appendix Appendix B):

$$\mathbb{E}[W(f_i, f_{-i})] \geq \tau(\Lambda, \underline{\Delta}) \gg 1 \text{ year} \tag{C.80}$$

which thereby completes the proof.

As a technical aside, the last computation requires a value for b, and we use $b = 6$. Moreover, for ease of computation, we use 0.99 as the fork probability even though $p > 0.99$. Note that Lemma 6 implies that the computation for a fork probability of 0.99 will produce a lower consensus wait time than that for $p > 0.99$ so that our computations can be seen as a lower bound. Finally, per Appendix Appendix B, the expected number of blocks to regain consensus, $\tilde{\tau}$, does not depend upon the block rate independently of the transaction rate. In turn, the overall consensus wait time decreases in the block rate for a given transaction rate and thus the consensus wait time is lowest when the block rate is highest. Since the block rate and block size are inversely proportional for a given transaction rate, the consensus wait time is lowest when the block size is minimized, so we set block sizes to unity for our computation. □

C4. Proofs for Sections 3 and 5

Proof of Proposition 2.. For all N, the following holds true:

$$\pi_* \leq \frac{\sup_{N\in\mathbb{N}} \pi_* N}{N} \tag{C.81}$$

In turn, invoking $\sup_{N\in\mathbb{N}} \pi_* N < \infty$ from Proposition 6 implies:

$$\limsup_{N\to\infty} \pi_* \leq \limsup_{N\to\infty} \frac{\sup_{N\in\mathbb{N}} \pi_* N}{N} = \lim_{N\to\infty} \frac{\sup_{N\in\mathbb{N}} \pi_* N}{N} = 0 \tag{C.82}$$

Finally, $\pi_* \in [0,1]$ for all N implies $\liminf_{N\to\infty} \pi_* \geq 0$ so that Eq. (C.82) implies $\lim_{N\to\infty} \pi_* = 0$, thereby completing the proof. □

Proof of Proposition 3.. For all N, the following holds true:

$$\pi_* \leq \frac{\sup_{N\in\mathbb{N}} \pi_* N}{N} \tag{C.83}$$

In turn, invoking $\sup_{N\in\mathbb{N}} \pi_* N < \infty$ from Proposition 7 implies:

$$\limsup_{N\to\infty} \pi_* \leq \limsup_{N\to\infty} \frac{\sup_{N\in\mathbb{N}} \pi_* N}{N} = \lim_{N\to\infty} \frac{\sup_{N\in\mathbb{N}} \pi_* N}{N} = 0 \tag{C.84}$$

Finally, $\pi_* \in [0,1]$ for all N implies $\liminf_{N\to\infty} \pi_* \geq 0$ so that Eq. (C.84) implies $\lim_{N\to\infty} \pi_* = 0$, thereby completing the proof. □

Proof of Proposition 4.. Lemma 8 yields:

$$\tau(\Lambda_N, \Delta(M)) \geq \frac{e^{\Lambda_N \Delta(M)} - 1}{\Lambda_N} \tag{C.85}$$

Note that $e^x - 1 = \sum_{n=1}^{\infty} \frac{x^n}{n!}$ so that $e^x - 1 \geq \frac{x^2}{2} + x$ when $x \geq 0$. In turn, Eq. (C.85) implies:

$$\tau(\Lambda_N, \Delta(M)) \geq \frac{\Lambda_N \Delta(M)^2}{2} + \Delta(M) \tag{C.86}$$

From Proposition 1 v, $M \geq \frac{B}{\beta} > 1$ so that $\Delta(M) \geq \Delta(\frac{B}{\beta}) > \Delta(1) = 0$. As a consequence, Eq. (C.86) further implies:

$$\tau(\Lambda_N, \Delta(M)) \geq \frac{\Lambda_N \Delta(\frac{B}{\beta})^2}{2} + \Delta(\frac{B}{\beta}) \tag{C.87}$$

so that taking $N \to \infty$ on both sides implies $\lim_{N\to\infty} \tau(\Lambda_N, \Delta(M)) = \infty$ as desired. □

Proof of Proposition 5.. We provide a constructive proof. In particular, we explicitly specify Λ_N such that there exists a full adoption equilibrium for all sufficiently large N (i.e., there exists $\underline{N} > 0$ such that $\pi_* = 1$ for all $N > \underline{N}$ and thus $\lim_{N\to\infty} \pi_* = 1 > 0$) and the mining network size diverges (i.e., $\lim_{N\to\infty} M = \infty$).

We specify the transaction rate as follows: $\Lambda_N = \frac{N-1}{2}$. Note that $\Delta(M) = 0$ implies $\Psi(\Lambda_N, \Delta(M)) = \frac{1}{\Lambda_N}$. Then, via Proposition 1 (D), a full adoption equilibrium exists if:

$$R_1 \cdot N^\alpha + R_0 \geq \frac{\bar{c}}{\Lambda_N} + (N-1)\frac{\bar{c} + \underline{c}}{2\Lambda_N} = \frac{2 \cdot \bar{c}}{N-1} + \bar{c} + \underline{c} \tag{C.88}$$

Note that:

$$\lim_{N\to\infty} \left(R_1 \cdot N^\alpha + R_0 - \frac{2 \cdot \bar{c}}{N-1} - \bar{c} - \underline{c} \right) = \infty \tag{C.89}$$

which implies that Eq. (C.88) is satisfied for all N sufficiently large. In turn, via Proposition 1 (C), there exists an $\underline{N} > 0$ such that $\pi_* = 1$ for all $N > \underline{N}$ as desired.

To complete the proof, we must demonstrate only that $\lim_{N\to\infty} M = \infty$. Proposition 1 (B) yields:

$$M = M(c_*) = \frac{B}{\beta} + \frac{N(N-1)}{6\beta\Lambda_N} \frac{(c_* - \underline{c}) \cdot (c_*^2 + c_*\underline{c} - 2\underline{c}^2)}{(\bar{c} - \underline{c})^2} \tag{C.90}$$

Then, using $\Lambda_N = \frac{N-1}{2}$ and $\pi_* = 1 \Leftrightarrow c_* = \bar{c}$ for $N > \underline{N}$, Eq. (C.90) becomes:

$$M = M(\bar{c}) = \frac{B}{\beta} + \frac{N}{3\beta} \cdot \frac{\bar{c}^2 + \bar{c}\underline{c} - 2\underline{c}^2}{\bar{c} - \underline{c}} \tag{C.91}$$

for $N > \underline{N}$. Finally, taking $N \to \infty$ in Eq. (C.91) yields:

$$\lim_{N\to\infty} M = \lim_{N\to\infty} \left(\frac{B}{\beta} + \frac{N}{3\beta} \cdot \frac{\bar{c}^2 + \bar{c}\underline{c} - 2\underline{c}^2}{\bar{c} - \underline{c}} \right) = \infty \tag{C.92}$$

which completes the proof. □

Proof of Proposition 9.. Either $R_1 \cdot N^\alpha + R_0 \geq \bar{c} \cdot \Psi(\Lambda, \Delta_C(M(\bar{c}))) + (N-1) \times \frac{\bar{c}+\underline{c}}{2\Lambda}$ or $R_1 \cdot N^\alpha + R_0 < \bar{c} \cdot \Psi(\Lambda, \Delta_C(M(\bar{c}))) + (N-1) \times \frac{\bar{c}+\underline{c}}{2\Lambda}$. We proceed by proving our result for each case in turn.

Case 1: $R_1 \cdot N^\alpha + R_0 \geq \bar{c} \cdot \Psi(\Lambda, \Delta_C(M(\bar{c}))) + (N-1) \times \frac{\bar{c}+\underline{c}}{2\Lambda}$

In this case, Proposition 1 (D) implies that $\pi_*^C = 1$ so that $\pi_*^C \geq \pi_*^D$ follows trivially from $\pi_*^D \in [0,1]$ since $\pi_*^D \leq 1 = \pi_*^C$.

Case 2: $R_1 \cdot N^\alpha + R_0 < \bar{c} \cdot \Psi(\Lambda, \Delta_C(M(\bar{c}))) + (N-1) \times \frac{\bar{c}+\underline{c}}{2\Lambda}$

Note that Proposition 1 implies that $\pi_*^C < 1$ in this case. Moreover, note that Lemma 9 implies that:

$$\bar{c} \cdot \Psi(\Lambda, \Delta_C(M(\bar{c}))) + (N-1) \times \frac{\bar{c}+\underline{c}}{2\Lambda} \leq \bar{c} \cdot \Psi(\Lambda, \Delta_D(M(\bar{c}))) + (N-1) \times \frac{\bar{c}+\underline{c}}{2\Lambda} \tag{C.93}$$

so that:

$$R_1 \cdot N^\alpha + R_0 < \bar{c} \cdot \Psi(\Lambda, \Delta_D(M(\bar{c}))) + (N-1) \times \frac{\bar{c}+\underline{c}}{2\Lambda} \tag{C.94}$$

and thus Proposition 1 also implies that $\pi_*^D < 1$. More explicitly, Proposition 1 (C) implies that $\pi_*^D = \frac{c_*^D - \underline{c}}{\bar{c} - \underline{c}}$ where c_*^D solves the following equation:

$$R_1 \cdot (\frac{c_*^D - \underline{c}}{\bar{c} - \underline{c}})^\alpha \cdot N^\alpha + R_0 = c_*^D \Psi(\Lambda, \Delta_D(M(c_*^D))) + \frac{N-1}{\bar{c} - \underline{c}} \times \frac{(c_*^D)^2 - \underline{c}^2}{2\Lambda} \tag{C.95}$$

Lemma 9 implies:

$$c_*^D \Psi(\Lambda, \Delta_D(M(c_*^D))) + \frac{N-1}{\bar{c} - \underline{c}} \times \frac{(c_*^D)^2 - \underline{c}^2}{2\Lambda} > c_*^D \Psi(\Lambda, \Delta_C(M(c_*^D))) + \frac{N-1}{\bar{c} - \underline{c}} \times \frac{(c_*^D)^2 - \underline{c}^2}{2\Lambda} \tag{C.96}$$

so that Eq. (C.95) becomes:

$$R_1 \cdot \left(\frac{c_*^D - \underline{c}}{\bar{c} - \underline{c}} \right)^\alpha \cdot N^\alpha + R_0 > c_*^D \Psi(\Lambda, \Delta_C(M(c_*^D))) + \frac{N-1}{\bar{c} - \underline{c}} \times \frac{(c_*^D)^2 - \underline{c}^2}{2\Lambda} \tag{C.97}$$

In turn, we define:

$$\Xi(x) \equiv R_1 \cdot (\frac{x - \underline{c}}{\bar{c} - \underline{c}})^\alpha \cdot N^\alpha + R_0 - \left(c_* \Psi(\Lambda, \Delta_C(M(x))) + \frac{N-1}{\bar{c} - \underline{c}} \times \frac{x^2 - \underline{c}^2}{2\Lambda} \right) \tag{C.98}$$

so that Eq. (C.97) is equivalent to $\Xi(c_*^D) > 0$. Note that the hypothesis of Case 2 (i.e., $R_1 \cdot N^\alpha + R_0 < \bar{c} \cdot \Psi(\Lambda, \Delta_C(M(\bar{c}))) + (N-1) \times \frac{\bar{c}+\underline{c}}{2\Lambda}$) is equivalent to $\Xi(\bar{c}) < 0$. Then, $\Xi(c_*^D) > 0$, $\Xi(\bar{c}) < 0$ and Ξ being continuous implies there exists an $x_* \in (c_*^D, \bar{c})$ such that $\Xi(x_*) = 0$. Further, Proposition 1 (C) establishes that $\Xi(x_*) = 0$ implies $c_*^C = x_* > c_*^D$ where the associated adoption cut-off is given by $\pi_*^C = \frac{c_*^C - \underline{c}}{\bar{c} - \underline{c}}$. Finally, $\pi_*^k = \frac{c_*^k - \underline{c}}{\bar{c} - \underline{c}}$ for $k \in \{C, D\}$ implies $\pi_*^C > \pi_*^D$, thereby completing the proof. □

Proof of Proposition 10.. We provide a constructive proof. In particular, we explicitly specify Λ_N such that there exists a full adoption equilibrium for all sufficiently large N (i.e., there exists $\underline{N} > 0$ such that $\pi_* = 1$ for all $N > \underline{N}$ and thus $\lim\limits_{N\to\infty} \pi_* = 1 > 0$) and the network size diverges (i.e., $\lim\limits_{N\to\infty} M = \infty$).

Recall that $\Psi(\Lambda_N, \Delta(M)) = \frac{1}{\Lambda_N} + \tau(p_F(\Lambda_N, \Delta(M)), \Lambda_N)$ where $\tau(p_F(\Lambda_N, \Delta(M)), \Lambda_N)$ is defined in Appendix Appendix B and discussed after the proof of Lemma 7. Note that we are not using Bitcoin's fork probability function and rather using a fork probability function as given by the hypothesis of this proposition (i.e., p_F such that $\sup\limits_{\Lambda,\Delta} p_F(\Lambda, \Delta) < 1$). Then, via Proposition 1 (D), a full adoption equilibrium exists if:

$$R_1 \cdot N^\alpha + R_0 \geq \bar{c} \times \left(\frac{1}{\Lambda_N} + \tau(p_F(\Lambda_N, \Delta(M)), \Lambda_N) \right) + (N-1) \frac{\bar{c}+\underline{c}}{2\Lambda_N} \tag{C.99}$$

We select the transaction rate to vary according to $\Lambda_N = \frac{N-1}{2}$, which implies that Eq. (C.99) becomes:

$$R_1 \cdot N^\alpha + R_0 \geq \bar{c} \times \left(\frac{1}{\Lambda_N} + \tau(p_F(\Lambda_N, \Delta(M)), \Lambda_N) \right) + \bar{c} + \underline{c} \tag{C.100}$$

Then, Lemma 7 yields that $\lim\limits_{N\to\infty} \tau(p_F(\Lambda_N, \Delta(M)), \Lambda_N) = 0$ so that:

$$\lim_{N\to\infty} \left(R_1 \cdot N^\alpha + R_0 - \bar{c} \times \left(\frac{1}{\Lambda_N} + \tau(p_F(\Lambda_N, \Delta(M)), \Lambda_N) \right) - \bar{c} - \underline{c} \right) = \infty \tag{C.101}$$

which implies that Eq. (C.99) is satisfied for all N sufficiently large. In turn, via Proposition 1 (C), there exists an $\underline{N} > 0$ such that $\pi_* = 1$ for all $N > \underline{N}$ as desired.

To complete the proof, we must demonstrate only that $\lim\limits_{N\to\infty} M = \infty$. Proposition 1 (B) yields:

$$M = M(c_*) = \frac{B}{\beta} + \frac{N(N-1)}{6\beta\Lambda_N} \frac{(c_* - \underline{c}) \cdot (c_*^2 + c_*\underline{c} - 2\underline{c}^2)}{(\bar{c} - \underline{c})^2} \tag{C.102}$$

Then, using $\Lambda_N = \frac{N-1}{2}$ and $\pi_* = 1 \Leftrightarrow c_* = \bar{c}$ for $N > \underline{N}$, Eq. (C.102) becomes:

$$M = M(\bar{c}) = \frac{B}{\beta} + \frac{N}{3\beta} \cdot \frac{\bar{c}^2 + \bar{c}\underline{c} - 2\underline{c}^2}{\bar{c} - \underline{c}} \tag{C.103}$$

for $N > \underline{N}$. Finally, taking $N \to \infty$ in Eq. (C.103) yields:

$$\lim_{N\to\infty} M = \lim_{N\to\infty} \left(\frac{B}{\beta} + \frac{N}{3\beta} \cdot \frac{\bar{c}^2 + \bar{c}\underline{c} - 2\underline{c}^2}{\bar{c} - \underline{c}} \right) = \infty \tag{C.104}$$

which completes the proof. □

References

Alsabah, H., Capponi, A., 2021. Pitfalls of Bitcoin's Proof-of-Work: R&D Arms Race and Mining Centralization. Working Paper.

Biais, B., Bisiére, C., Bouvard, M., Casamatta, C., 2019. The blockchain folk theorem. Rev. Financ. Stud. 32 (5), 1662–1715.

Biais, B., Bisiére, C., Bouvard, M., Casamatta, C., Menkveld, A.J., 2020. Equilibrium Bitcoin Pricing. Working Paper.

Castro, M., Liskov, B., et al., 1999. Practical byzantine fault tolerance. In: OSDI, vol. 99, pp. 173–186.

Chiu, J., Koeppl, T.V., 2020. The Economics of Cryptocurrencies - Bitcoin and Beyond. Working Paper.

Chung, F., Lu, L., 2002. The average distances in random graphs with given expected degrees. Proc. Natl. Acad. Sci. 99 (25), 15879–15882.

Cong, L.W., He, Z., Li, J., 2021. Decentralized mining in centralized pools. Rev. Financ. Stud. 34, 1191–1235.

Cong, L.W., Li, Y., Wang, N., 2021. Tokenomics: dynamic adoption and valuation. Rev. Financ. Stud. 34, 1105–1155.

Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E.G., et al., 2016. On scaling decentralized blockchains. In: International Conference on Financial Cryptography and Data Security. Springer, pp. 106–125.

Decker, C., Wattenhofer, R., 2013. Information propagation in the bitcoin network. In: IEEE P2P 2013 Proceedings.

Easley, D., O'Hara, M., Basu, S., 2019. From mining to markets: the evolution of bitcoin transaction fees. J. Financ. Econ. 134 (1), 91–109. doi:10.1016/j.jfineco.2019.03.004.

Eyal, I., Gencer, A.E., Sirer, E.G., van Renesse, R., 2015. Bitcoin-NG: a scalable blockchain protocol. CoRR. abs/1510.02037.

Ferreira, D., Li, J., Nikolowa, R., 2020. Corporate Capture of Blockchain Governance. Working Paper.

Foley, S., Karlsen, J.R., Putnins, T.J., 2019. Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies? Rev. Financ. Stud. 32 (5), 1798–1853.

Griffin, J.M., Shams, A., 2020. Is bitcoin really un-tethered? J. Finance 75, 1913–1964.

Huberman, G., Leshno, J.D., Moallemi, C., 2021. Monopoly without a monopolist: an economic analysis of the bitcoin payment system. Rev. Econ. Stud. doi:10.1093/restud/rdab014.

Iyengar, G., Saleh, F., Sethuraman, J., Wang, W., 2022. Economics of Permissioned Blockchain Adoption. Working Paper. Columbia University.

John, K., O'Hara, M., Saleh, F., 2022. Bitcoin and beyond. Annu. Rev. Financ. Econ. 14.

Lehar, A., Parlour, C., 2020. Miner Collusion and the Bitcoin Protocol. Working Paper.

Makarov, I., Schoar, A., 2020. Trading and arbitrage in cryptocurrency markets. J. Financ. Econ. 135 (2), 293–319.

Nakamoto, S., 2008. Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S., 2016. Bitcoin and Cryptocurrency Technologies. Princeton University Press.

Pagnotta, E., 2022. Bitcoin as decentralized money: prices, mining rewards, and network security. Rev. Financ. Stud.. Forthcoming

Pass, R., Shi, E., 2018. Thunderella: blockchains with optimistic instant confirmation. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, pp. 3–33.

Raskin, M., Saleh, F., Yermack, D., 2019. How Do Private Digital Currencies Affect Government Policy? NBER Working Paper.

Riordan, O., Wormald, N., 2010. The diameter of sparse random graphs. Comb. Probab. Comput. 19, 835–926.

Saleh, F., 2019. Volatility and Welfare in a Crypto Economy. Working Paper.

Saleh, F., 2021. Blockchain without waste: proof-of-stake. Rev. Financ. Stud. 34, 1156–1190.

de Vries, A., 2018. Bitcoin's growing energy problem. Joule 2 (5), 801–805.

Yermack, D., 2015. Is bitcoin a real currency? An economic appraisal. Handb. Digit. Currency 31–43.

Zhou, Q., Huang, H., Zheng, Z., Bian, J., 2020. Solutions to scalability of blockchain: a survey. IEEE Access 8, 16440–16455.