Bitcoin's Fatal Flaw: The Limited Adoption Problem*

Franz J. Hinzen[†] Kose John[‡] Fahad Saleh[§]

December 17, 2019

Abstract

Bitcoin remains sparsely adopted even a decade after its birth. We demonstrate theoretically that this limited adoption arises as an equilibrium outcome rather than as a transient feature. Our results arise primarily because Bitcoin's design precludes expanding supply as a response to heightened demand. We demonstrate that expanding supply prolongs Bitcoin's consensus process, thereby generating a dilemma. Either supply does not keep pace with demand so that prohibitive delays arise for traditional reasons, or supply keeps pace with demand and prohibitive delays arise due to the prolonged consensus process. In either case, prohibitive delays generate limited adoption as an equilibrium outcome. We also demonstrate that permissioned blockchains may obtain widespread adoption, thereby highlighting the need for research on alternatives to Bitcoin.

Keywords: Bitcoin, Blockchain, Proof-of-Work, Limited Adoption, Payment Systems, FinTech

JEL Classification: E42, G00, G29

---

*This paper previously circulated under the title, "Proof-of-Work's Limited Adoption Problem." We thank Anup Agrawal, Yakov Amihud, Daniel Andrei, Jaroslav Borovicka, Matthieu Bouvard, Agostino Capponi, William Cong, Sean Foley, Manasa Gopal, Hanna Halaburda, Joel Hasbrouck, Sabrina Howell, Gur Huberman, Felix Irresberger, Ari Juels, Steven Kou, Doron Levit, Jiasun Li, Laura Xiaolei Liu, Evgeny Lyandres, Bryan Routledge, Zhan Shi, Chester Spatt, Charles Trzcinka, Warren Weber, Danxia Xie, Baozhong Yang, David Yermack, Zhen Zhou, seminar participants at McGill University, NYU Stern, Peking University, Tsinghua PBC School of Finance, Tsinghua School of Social Sciences and conference participants at the First New York Fed Research Conference on FinTech, the 2019 Eastern Finance Association meeting, the 2019 Financial Management Association meeting, the 2019 Financial System of the Future Conference, the 2019 Conference on Financial Economics and Accounting and the 2019 Philadelphia Federal Reserve FinTech Conference for valuable comments.

[†]New York University Stern School of Business. Email: fhinzen@stern.nyu.edu

[‡]New York University Stern School of Business. Email: kjohn@stern.nyu.edu

[§]McGill University Desautels School of Management. Email: fahad.saleh@mcgill.ca

1 Introduction

A question remains whether Bitcoin's limited usage arises due to its youth or because of its underlying economic structure. This paper answers that question by demonstrating that limited adoption constitutes an endogenous characteristic of not only Bitcoin but also Proof-of-Work (PoW) payments blockchains more generally. We demonstrate that the economics of decentralized PoW payments blockchains make limited adoption an inescapable equilibrium outcome. Our critique does not apply to all blockchains. In fact, our analysis explicitly demonstrates that permissioned blockchains may overcome limited adoption. Recently, that insight has become particularly salient with the announcement of Libra, a cryptocurrency with the explicit goal of becoming "as widely accepted... as possible."[1] Our analysis does not explicitly endorse any particular project; rather, our work highlights the need for research on alternatives to Bitcoin in the nascent field of blockchain economics.

Our key insights rely upon the existence of negative network effects within PoW payments blockchains. These negative network effects distinguish PoW payments blockchains from traditional payment systems and serve as the central economic force that generates limited adoption. To understand why negative network effects might arise, we emphasize that a blockchain constitutes a unique electronic ledger that is stored among a potentially large network of agents. For a PoW blockchain, ledger updates arrive randomly and to random agents within the network so that periodic inconsistencies necessarily arise. If the PoW protocol fails to expediently reconcile those inconsistencies, then prohibitive wait times would arise which would in turn lead users to abandon the platform. Our analysis highlights that the PoW reconciliation process becomes prolonged as the network size expands, thereby generating delays and limited adoption.

We refer to the agents that store the ledger as validators.[2] Our key results highlight

[1] Source: https://libra.org/en-US/vision/#how_it_works

[2] Validators on a PoW blockchain are typically called miners. We use the more general term, val-

that limited adoption arises for a decentralized PoW blockchain even if validators attempt to coordinate to reconcile ledger inconsistencies (Propositions 4.3 and 4.5). Our results arise because agreement among multiple agents requires communication, and communication requires strictly positive time. Thus, irrespective of validator incentives, decentralization imposes a constraint on the ability of validators to coordinate. Subsequently, we explain how that constraint can lead to limited adoption.

We model a PoW payments blockchain as a queue in which PoW validators service a set of users. Each user has a unit transaction demand and derives utility from that transaction being settled on the blockchain. Users have a heterogeneous dis-utility for waiting. Each user may pay a fee to reduce her expected wait time. Each user also dislikes paying a fee. Therefore, she selects a fee in equilibrium to optimally balance her dislike for waiting with that of paying a fee. We also allow for an outside option so that a user may abandon the blockchain entirely if her maximal utility from using the blockchain is below a reservation level. This outside option reflects the fact that a potential PoW blockchain user may opt to transact via a traditional payment system (e.g., credit card, debit card, etc...).

Our first main result (Proposition 4.3) highlights that PoW payments blockchains cannot sustain a non-negligible proportion of potential users when the number of potential users becomes large. This result highlights Bitcoin's inability to compete with traditional payment systems like Visa. Most economic agents may not consider Bitcoin as an alternative, but our result highlights that even if the approximately 150 million daily Visa users considered Bitcoin as an option, only a trivial fraction of them would choose to adopt Bitcoin.

We relate the aforementioned result to three features of PoW payments blockchains: the need for agreement, the blockchain's permissionless nature, and the fixed rate of

idator, because we also study permissioned blockchains within this paper. In a permissioned setting, validators are typically not referred to as miners.

service. The need for agreement, hereafter referred to as *consensus*, arises because the blockchain is a unique ledger, and disagreement contradicts the uniqueness. Consensus makes communication time across the network, hereafter referred to as *network delay*, a crucial feature of our model.[3] The blockchain's permissionless nature refers to the fact that PoW blockchains do not restrict the set of agents that may serve as validators. Economically, this lack of a restriction corresponds to free entry into the PoW validator network. As previously noted, users may pay fees to reduce wait times. Those fees are paid to validators, and potential validators trade off the benefits from accruing those fees against the costs of participating in the validation process. Therefore, the validator network arises endogenously. The fixed rate of service refers to an observed fact of Bitcoin and other prominent PoW blockchains. Bitcoin receives a block approximately every 10 minutes. This fixed rate of service corresponds to a supply constraint on the number of transactions per unit time because each block has a fixed capacity.

Proposition 4.3 arises from a straight-forward economic analysis. The fixed rate of service implies that prices rather than quantities respond to positive demand shocks. Thus, an increase in transaction demand endogenously generates an increase in fees (i.e., the price for faster service). That fee increase in turn increases revenues from validating. The blockchain's permissionless nature implies that these increased revenues induce validators to enter the PoW network. The PoW 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 the blockchain towards traditional payment systems so that the blockchain maintains only users relatively insensitive to wait times. Accordingly, Proposition 4.3 establishes that PoW payments blockchains cannot maintain a non-negligible payments market share when facing heightened demand - we term this problem the *limited adoption problem*.

In a traditional setting, that problem possesses a simple solution: expand supply to

[3] Section 2 provides context regarding network delay.

meet demand. For example, a grocery store facing a sudden burst of customers checking out (i.e., heightened demand) responds by increasing the number of check-out counters (i.e., expanded supply). Our second main result (Proposition 4.5) highlights that this traditional solution of expanding supply (i.e., increasing the blockchain's service rate) to meet demand fails to resolve the problem in a decentralized PoW blockchain setting.

To understand this finding, we emphasize that the need for consensus does not arise in traditional settings. In the context of the previously referenced grocery store example, cashiers at each check-out counter do not need to agree upon a unique order of customers served across all cashiers. If cashiers did need such agreement to check-out customers then wait times would also include the time elapsed to secure such agreement and that time would likely increase with the number of cashiers.

The blockchain's consensus process eventually lengthens as its service rate increases. That result arises because a higher service rate implies that each validator is more likely to complete service sooner. Then, the likelihood that a given validator completes service before receiving news of an earlier service by another validator increases with the service rate so that validators are more likely to disagree on the order of events when the blockchain expands supply. The increased likelihood of disagreement, in turn, prolongs the consensus process and precludes expansion of supply as a solution for heightened demand in the case of a decentralized PoW blockchain.

The previous discussion establishes a dilemma that separates a decentralized PoW blockchain from a traditional payment system. Both systems face limited adoption if supply does not expand to meet demand. However, a traditional payment system may expand supply to meet demand and thereby overcome limited adoption. A decentralized PoW blockchain, however, faces an elongated consensus process when expanding supply and thus faces limited adoption even if supply expands to meet demand. A PoW blockchain may overcome the referenced dilemma only if the validator network degenerates to a single member as such a case trivializes the consensus process and thereby allows an expansion of supply to resolve limited adoption as in a traditional setting.

The necessity of centralization to break PoW's limited adoption problem motivates us to consider permissioned blockchains. A permissioned blockchain offers a semi-centralized setting with neither an artificial supply constraint nor free entry among validators. We demonstrate that a permissioned blockchain induces lower payment confirmation times than a PoW blockchain and overcomes the limited adoption problem. Nonetheless, we acknowledge that a permissioned blockchain may not dominate a PoW blockchain because malicious validator behavior may arise in equilibrium for a permissioned blockchain. We, therefore, turn to examining validator incentives for this class of blockchains.

We begin by analyzing a standard majority rule consensus protocol. Such a protocol creates a coordination game with multiple equilibria. All validators behave honestly in one equilibrium and maliciously in another equilibrium. These results arise because a validator gains from successfully attacking the blockchain but faces a reputation cost from an unsuccessful attack. The majority-rule consensus protocol thus raises security concerns for a permissioned blockchain.

To resolve the aforementioned concerns, we propose an alternative consensus protocol. That protocol weights votes by each validators' stake in the cryptocurrency native to the blockchain. Such a protocol aligns validator incentives in a way that precludes malicious validator behavior. Validators internalize that prices negatively reflect the probability that the blockchain incurs a successful attack. An attack equilibrium cannot exist because validators respond optimally to a potential attack by acquiring a stake in the cryptocurrency sufficiently large to become marginal and thwart the attack.

A permissioned blockchain with a stake-based consensus protocol escapes the limited adoption problem and induces honest validator behavior. This has important implications for the introduction of blockchain as a payment system. While PoW may not be viable due to the limited adoption problem, a well-designed permissioned alternative may be suitable for widespread adoption. Notably, Facebook recently announced plans for a permissioned blockchain with the explicit goal of widespread adoption. While we demonstrate that permissioned blockchains may overcome limited adoption, our results do not demonstrate that arbitrary implementations of permissioned blockchains necessarily obtain widespread adoption.

This paper relates to a large literature that studies PoW economics and cryptoassets. Eyal and Sirer (2014), Nayak, Kumar, Miller, and Shi (2015), Carlsten, Kalodner, Weinberg, and Narayanan (2016), Cong, He, and Li (2018), Alsabah and Capponi (2019) and Biais, Bisière, Bouvard, and Casamatta (2019) analyze PoW mining strategies. Huberman, Leshno, and Moallemi (2019) and Easley, O'Hara, and Basu (2019) analyze transaction fees and wait times for users under a PoW protocol. Foley, Karlsen, and Putnins (2019) examine the extent to which cryptocurrencies facilitate illegal activities. Raskin, Saleh, and Yermack (2019) analyze the relationship between private digital currencies and government policy. Kroeger and Sarkar (2017), Biais, Bisière, Bouvard, Casamatta, and Menkveld (2018), Liu and Tsyvinski (2018), Makarov and Schoar (2019), Pagnotta and Buraschi (2018), Li, Shin, and Wang (2019b) and Shams (2019) study the determinants of cryptoasset prices. Other notable works include Gandal and Halaburda (2016), Harvey (2016), Chiu and Koeppl (2017), Abadi and Brunnermeier (2018), Griffin and Shams (2018), Jermann (2018) and Chiu and Koeppl (2019) and Fernández-Villaverde and Sanches (2019).

This paper highlights an important shortcoming of PoW payments blockchains. In doing so, our work adds to the literature that highlights PoW's economic limitations. Budish (2018) argues that the possibility of an attack limits Bitcoin's economic size. Yermack (2015) documents exorbitant bitcoin price volatility. Pagnotta (2018) and Saleh (2019b) theoretically demonstrate that PoW contributes to that price volatility; Saleh (2019b) also demonstrates that PoW induces welfare losses.

This paper also contributes to a growing literature that considers alternatives to PoW payments blockchains. We provide one of the first analyses of permissioned blockchains and show that a properly designed consensus protocol yields desirable validator behavior. Akin to Falk and Tsoukalas (2018), we consider voting in a blockchain context, but we focus on validator voting in a public permissioned setting whereas Falk and Tsoukalas (2018) examine token-weighted voting for crowd-sourcing of information. Cao, Cong, and Yang (2018) and Chod, Trichakis, Tsoukalas, Aspegren, and Weber (2018) predate our work and also study permissioned blockchains but for auditing and supply chain purposes respectively. Sockin and Xiong (2018), Tinn (2018), Cong and He (2019), Cong, Li, and Wang (2019a), Cong, Li, and Wang (2019b), Gryglewicz, Mayer, and Morellec (2019) and Mayer (2019) depart from the Bitcoin paradigm by examining a blockchain platform that possesses functionality beyond payment processing. Hinzen, Irresberger, John, and Saleh (2019) provide an overview and an organizing empirical framework for the public blockchain ecosystem. Chod and Lyandres (2018), Lee, Li, and Shin (2018), Li and Mann (2018), Malinova and Park (2018), Catalini and Gans (2019), Gan, Tsoukalas, and Netessine (2019), Davydiuk, Gupta, and Rosen (2019) and Howell, Niessner, and Yermack (2019) study initial coin offerings. Basu, Easley, O'Hara, and Sirer (2019) propose an alternative fee setting mechanism to that employed by Bitcoin. Saleh (2019a) formally analyzes Proof-of-Stake (PoS) and establishes that such a protocol induces consensus under certain conditions. Fanti, Kogan, and Viswanath (2019) provide a valuation framework for PoS payments systems. Rosu and Saleh (2019) study the evolution of shares in a PoS cryptocurrency. Liu, Tsyvinski, and Wu (2019) study cryptoasset risk factors in general and find novel empirical evidence highlighting that more cost-efficient cryptoassets possess better return characteristics than PoW cryptoassets.

Also notable, there exists a large literature within computer science that studies security of various blockchain protocols. Prominent papers within that literature include Miller and LaViola (2014), Chen and Micali (2016), Kiayias, Russell, David, and

Oliynykov (2017) and Daian, Pass, and Shi (2019). Our paper differs from those works in that we do not establish security of any permissionless protocol. Rather, we assume security of PoW and establish limited adoption despite this generous assumption. Our paper also analyzes security of a permissioned blockchain protocol. However, our notion of security equates with incentive compatibility of validators, whereas the computer science security notion equates to robustness in the presence of an exogenously motivated attacker.

This paper proceeds as follows. Section 2 discusses relevant institutional details. Section 3 presents the PoW model, defines a PoW Equilibrium and establishes both existence and uniqueness of such an equilibrium. Section 4 analyzes payment confirmation times and formalizes the limited adoption problem. Section 5 discusses permissioned blockchains and offers a stake-based consensus protocol as an alternative to PoW. Section 6 concludes. All proofs appear in Appendix B.

2 Institutional Background

For a block to enter a PoW blockchain, that block must solve a puzzle. Hereafter, we refer to that puzzle as the PoW puzzle and any block that solves the PoW puzzle as a valid block. Being valid constitutes a necessary, but not a sufficient condition, for a block to enter the blockchain. Block validity is not a sufficient condition due to PoW's permissionless nature which requires that any validator may propose a block. If multiple validators propose valid blocks at the same height, then only one such block may enter the blockchain, thereby precluding block validity as a sufficient condition for a block to enter the blockchain.

Validators may propose valid blocks at the same height for various reasons. Biais et al. (2019) consider such events arising from validator incentives. We abstract from validator incentives and assume validators attempt to coordinate on a single chain. A key ingredient of our model is that, even with such a generous security assumption, multiple blocks may be proposed at the same height due to network delay. We show that network delay has grave economic implications that prevent PoW payments blockchains, such as Bitcoin, from becoming widely adopted.

Network delay refers to the time required for information to travel across the network. The presence of network delay implies that validators may perceive different longest chains at a given point in time. If Validator A proposes a valid block at a given height, other validators may nonetheless continue searching for a valid block at that same height, because news of Validator A's valid block has not propagated through the entire network. With a positive probability, some other validator, Validator B, may find a valid block before receiving news regarding Validator A's valid block. Then, Validators A and B perceive different blockchains which we refer to as a fork.

The propensity of such forks arising thus depends on the extent of network delay which in turn is a function of the structure of the validator network. Since PoW blockchains are permissionless, such blockchains generally adopt a random network topology in which case network delay is approximately a logarithmic function of the number of nodes (see Chung and Lu (2002) and Riordan and Wormald (2010)). In our analysis, we specify network delay in more general terms so that a logarithmic function constitutes a special case. In practice, forks generated by network delay constitute the majority of forks arising on the Bitcoin blockchain (see Decker and Wattenhofer (2013)), yet the economics literature has largely ignored such forks. Although these forks arise for non-economic reasons, our work highlights that they possess significant economic implications in that they generate the limited adoption problem.

3 PoW Model

We model an economy that evolves in continuous time. Our model consists of a validator network that stores the blockchain and a finite number of potential blockchain users.

3.1 Users

Our model involves finitely many users, $i \in \{1, ..., N\}$. Each user possesses only one transaction. We model user preferences akin to Easley et al. (2019) and Huberman et al. (2019). At $t = 0$, User i learns her type, $c_i \sim U[0, 1]$. c_i denotes the delay cost for User i, which remains unknown to others.[4] After learning her type, User i selects a fee level, f_i, that solves the problem in (1) below.

$$\max_{f \geqslant 0} R - c_i \cdot \mathbb{E}[W(f, f_{-i}) \mid c_i] - f \tag{1}$$

$W(f, f_{-i})$ represents the wait time for User i's transaction to earn confirmation when User i pays f as a fee, while the other users pay fee f_{-i}. R represents the utility of User i having her transaction processed. If $\max_{f \geqslant 0} R - c_i \cdot \mathbb{E}[W(f, f_{-i}) \mid c_i] - f < 0$ then User i opts to transact via traditional payment systems rather than on the blockchain.

3.2 Validators

Because PoW blockchains admit free entry among validators, we determine the number of validators, V, endogenously. Each potential validator must pay some cost $\beta > 0$ to acquire validation technology and join the network. Each validating node represents a single processor, and we assume that each processor possesses identical hashing power so that each validator expects to earn an equal share of fees. We assume validators

[4]We model c_i as independent of all else.

possess risk-neutral preferences. Then, free entry yields Equation (2) with V being the equilibrium number of validators.

$$V = \frac{\mathbb{E}[\sum_i f_i]}{\beta} \tag{2}$$

For exposition, we assume that each block contains only one transaction.[5] We further assume that no coinbase transactions exist so that validators receive compensation exclusively through fees. Validators optimally service transactions in descending order of fees.

3.3 Blockchain

Blocks arrive according to a compound Poisson process with rate $\Lambda > 0$. We assume that each arrival occurs at a new block height, but we allow that network delay may yield multiple blocks at the same height. Multiple blocks at the same height constitute a fork and correspond to disagreement regarding the blockchain's content. A fork arises if different validators solve the same PoW puzzle before communicating with each other. Given an arrival at time t, a Poisson process with rate Λ produces at least one more arrival within the next Δ time units with probability $1 - e^{-\Lambda\Delta}$. Accordingly, we assume that an arrival corresponds to multiple blocks at a given height with probability $1 - e^{-\Lambda\Delta(V)}$. $\Delta(V)$ denotes the delay for a network of size V. We impose $\Delta(1) = 0$, $\lim_{V\to\infty} \Delta(V) = \infty$, and $\Delta'(V) > 0$ for $V > 1$.[6,7]

We assume that payments cannot be confirmed during a fork because, in such a case, validators disagree regarding the ledger's contents. We require that validators

[5] Decker and Wattenhofer (2013) establishes that network delay increases linearly in block size for non-trivial block sizes so that increasing block-rates and increasing block-sizes produce similar results. We allow arbitrary block-rates, so our results hold approximately for arbitrary block sizes.

[6] We model network delay in such generality to capture various potential validator network structures. Coordination may reduce network delay's sensitivity to network size, but our results nonetheless hold due to our general specification of $\Delta(V)$.

[7] $\Delta(V)$ lacks real-world meaning if $V \in [0, 1)$. Nonetheless, we specify $\forall V \in [0, 1) : \Delta(V) = 0$ for technical reasons. Our results do not depend upon this assumption.

must agree on $b \in \mathbb{N}_+$ consecutive blocks to restore agreement on the entire ledger's content. In the text, we focus upon $b = 1$, but we derive results more generally for arbitrary b. $b = 1$ corresponds to assuming that agreement on the entire ledger's content requires only agreement on the most recent block. In general, agreement on a single block need not imply agreement on the full chain. Thus, our findings highlight that limited adoption arises for a decentralized PoW blockchain even with generous security assumptions regarding the consensus process.

3.4 Equilibrium

Definition 3.1. PoW Equilibrium

A PoW Equilibrium is an entrant cut-off, $c^* \in [0, 1]$, a fee function, $\phi : [0, 1] \mapsto \mathbb{R}_+$, a set of fee choices, $\{f_i\}_{i=1}^N$, and a validator network size, $V \geqslant 0$, given a number of users, $N \geqslant 2$, a blockchain utility, $R > 0$, and a block arrival rate, $\Lambda > 0$, such that:

(i) $\forall i : \phi(c_i)$ solves the problem in (1) if $c_i \leqslant c^*$ and $\phi(c_i) = 0$ otherwise

(ii) $\forall i : c_i \leqslant c^* \Leftrightarrow \max\limits_{f \geqslant 0} R - c_i \cdot \mathbb{E}[W(f, f_{-i}) \mid c_i] - f \geqslant 0$

(iii) $\forall i : f_i = \phi(c_i)$

(iv) $W(f, f_{-i}) = \sum\limits_{j: f < f_j} H_j + H_i + Z_i, H_j \sim \exp(\Lambda), \mathbb{E}[Z_i] = \tau(\Lambda, V)$.

(v) $\beta V = \mathbb{E}[\sum\limits_{i} f_i]$.

Definition 3.1 characterizes the equilibrium. Without further reference, we assume that the blockchain's stationary distribution characterizes its initial state. The interested reader may consult Appendix A for the explicit stationary distribution and associated technical details. Condition 3.1 (i) asserts that users select an optimal fee schedule. Condition 3.1 (ii) states that a user transacts on the blockchain if and only if she derives weakly higher utility from transacting on the blockchain over the traditional payment systems. Condition 3.1 (iii) states that a user pays a fee only if she transacts on the blockchain. Condition 3.1 (iv) characterizes wait times as decomposed into three components; the wait for higher priority transactions, $\sum_{j:f<f_j} H_j$, for personal service, H_i, and for fork resolution, Z_i. Due to block arrival according to a compound Poisson process, wait times for individual blocks are independently and identically distributed following an exponential distribution with rate Λ. We let $\tau(\Lambda, V)$ denote the expected fork-resolution time and characterize this function explicitly in Appendix A. Condition 3.1 (v) imposes no profits for validators in equilibrium because free entry characterizes the validator network.

Proposition 3.1. *Existence and Uniqueness of a PoW Equilibrium*

There exists a PoW Equilibrium. There exists no other equilibrium for which ϕ constitutes a strictly increasing and differentiable function on the interval $(0, c^*)$. The following conditions characterize the equilibrium:

(A) $\phi(c_i) = (N-1)\frac{c_i^2}{2\Lambda}$ *if* $c_i \leqslant c^*$ *and* $\phi(c_i) = 0$ *otherwise*

(B) $R < \Psi(\Lambda, \frac{(N-1)N}{6\beta\Lambda}) + \frac{N-1}{2\Lambda} \implies R = c^*\Psi(\Lambda, V) + \frac{(c^*)^2(N-1)}{2\Lambda}$

(C) $R \geqslant \Psi(\Lambda, \frac{(N-1)N}{6\beta\Lambda}) + \frac{N-1}{2\Lambda} \implies c^* = 1$

(D) $\beta V = (N-1)N\frac{(c^*)^3}{6\Lambda}$.

Proposition 3.1 establishes existence and uniqueness of a PoW Equilibrium with $\Psi(\Lambda, V) \equiv \frac{1}{\Lambda} + \tau(\Lambda, V)$ denoting the expected wait time of the highest priority user. Proposition 3.1 (A) characterizes the equilibrium fee function. Proposition 3.1 (B) characterizes the entrant cut-off in the case that there exists a user indifferent between using the blockchain and a traditional alternative. Proposition 3.1 (C) characterizes the entrant cut-off in the case that all users weakly prefer transacting via the blockchain. Proposition 3.1 (D) characterizes the equilibrium number of validators.

4 PoW Results

Having established existence and uniqueness of a PoW Equilibrium, we turn to analyzing the properties of that equilibrium. Section 4.1 analyzes payment confirmation times. Section 4.2 establishes the limited adoption problem.

4.1 Payment Confirmation Times

We define $W_i \equiv \mathbb{E}[W(f_i, f_{-i}) \mid c_i]$ as the expected confirmation time for User i if she uses the blockchain. Equation (3) decomposes payment confirmation times into three parts.[8] $(N-1)\frac{(c^{*}-c_i)}{\Lambda}$ equals the expected service time for higher priority users. $\frac{1}{\Lambda}$ equals the expected service time for User i. $\tau(\Lambda, V)$ references the expected fork resolution time.

$$W_i = (N-1)\frac{(c^{*}-c_i)}{\Lambda} + \frac{1}{\Lambda} + \tau(\Lambda, V) \tag{3}$$

Fork resolution time constitutes a feature distinct from a traditional setting. This feature arises because blockchain payment confirmation requires agreement by all validators within the network. That agreement becomes harder to achieve when blocks arrive quickly relative to the time needed for a given validator to communicate her ledger to the network. Accordingly, disagreement arises more frequently as the network grows or as the block rate rises so that increasing the block rate need not expedite conformation times. In the absence of forks, confirmation times decrease as the block rate rises. Nonetheless, in the presence of forks, as the block rate rises so too does the fork frequency which counteracts the aforementioned effect.

Proposition 4.1. *Payment Confirmation Lower Bound*

Network delay bounds below all user payment confirmation times (i.e., $\forall i : W_i \geqslant$

[8] Equation (3) follows from Definition 3.1 (iv) and Proposition 3.1 (A)

$\tau(\Lambda, V) \geqslant \Delta(V))$.

Proposition 4.1 establishes that PoW induces network delay as a lower bound for confirmation times. Intuitively, a slow block rate yields a low fork frequency whereas a fast block rate yields a high fork frequency. Since forks delay validator agreement, arbitrarily fast payment confirmation cannot obtain for a decentralized PoW blockchain.

Proposition 4.2. *Arbitrarily Large Payment Confirmation Time*
All user payment confirmation times diverge as demand diverges, (*i.e.,* $\forall i : \lim_{N\to\infty} W_i = \infty$). *This result holds in particular for the marginal user* (*i.e.,* i *such that* $c_i = c^*$), *who is serviced with highest priority* (*i.e.,* $\forall j : f_i \geqslant f_j$).

Next, we turn our attention to how payment confirmation times vary with increases in transaction demand. Proposition 4.2 establishes that payment confirmation times diverge for all users, including the highest priority user, as transaction demand grows.[9]

A PoW blockchain imposes an artificial supply constraint via a fixed block rate. As transaction demand rises, the artifical supply constraint induces higher fees which in turn causes more validators to enter the network. The larger validator network increases network delay which in turn increases fork frequency and yields arbitrarily large payment confirmation times even for the highest priority user. Although the highest priority user receives service first (with probability one), her expected confirmation time diverges because expected fork resolution time diverges.

4.2 Limited Adoption Problem

The aforementioned prolonged payment confirmation times have important implications for the viability of a PoW payments blockchain. Specifically, a decentralized PoW payments blockchain cannot maintain a non-negligible market share when facing

[9] We refer to User i such that $c_i = c^*$ as the highest priority user. Any such user receives service first with probability one.

heightened demand. We first establish that result in a setting with a fixed rate of service (Proposition 4.3). That setting corresponds to the setting of major deployed PoW payments blockchains such as Bitcoin. We then establish that the result maintains even when allowing the blockchain's service rate to vary with demand (Proposition 4.5). The latter result distinguishes PoW payments blockchains from traditional payment systems because it establishes that the traditional solution of expanding supply to meet demand fails for a decentralized PoW blockchain.

Proposition 4.3. *Limited Adoption I*
Adoption decreases as demand rises (i.e., c^* decreases in N). Moreover, the blockchain faces limited adoption (i.e., $\lim_{N\to\infty} c^* = 0$).

Proposition 4.3 provides our first main result. This result establishes that PoW payments blockchains cannot maintain a non-negligible market share when facing heightened demand. This result highlights the inability of PoW payments blockchains such as Bitcoin to compete with traditional payment systems. If a large number of users considered Bitcoin as an alternative, only a trivial fraction of them would adopt the blockchain.

To understand Proposition 4.3, we offer some context on the economic channel. Section 4.1 demonstrates that increases in transaction demand eventually yield increases in expected confirmation times for all blockchain users. These increased payment confirmation times drive users from the blockchain to traditional payment systems. If the blockchain sustains a large volume, then congestion induces fees which leads to validator entry. That validator entry prolongs payment confirmation times and thereby drives away all but the most dogmatic blockchain fanatics (i.e., Users i such that $c_i \leqslant c^*$). Therefore, PoW payments blockchains such as Bitcoin cannot obtain widespread adoption; rather, limited adoption constitutes an intrinsic and endogenous characteristic of such blockchains.

Proposition 4.4. *Endogenous Network Delay*

Let c_v^* *denote the adoption rate of a network with variable network delay that satisfies the regularity discussed within Section 3. Let* c_c^* *denote the adoption rate of a network with constant network delay. Then,* $c_v^* < c_c^*$ *for large transaction demands (i.e.,* $\exists \underline{N} : \forall N > \underline{N} : c_v^* < c_c^*$*).*

Network delay and the fact that it may endogenously grow plays an important role in our analysis. To highlight that role, we compare adoption associated with a variable network delay function to that associated with a constant network delay function via Proposition 4.4. Proposition 4.4 establishes that adoption for a network with constant delay eventually dominates that for a network with variable delay. The constant network delay may initially exceed the variable network delay, but network size diverges with transaction demand so that the variable nature of network delay in practice (see Chung and Lu (2002) and Riordan and Wormald (2010)) exacerbates the limited adoption problem.

Proposition 4.5. *Limited Adoption II*

For exposition, we assume that $\lim_{N\to\infty} c^*$ *exist. The blockchain necessarily faces either centralization (i.e.,* $\limsup_{N\to\infty} V \leqslant 1$*) or limited adoption (i.e.,* $\lim_{N\to\infty} c^* = 0$*).*

Within a traditional setting, heightened demand need not induce limited adoption precisely because supply may expand to meet the heightened demand. In the PoW blockchain setting, expanding supply corresponds to increasing the block service rate (i.e., increasing Λ). Our second main result (Propostion 4.5) considers such a solution and finds that this approach succeeds only in so far as it induces centralization. This finding arises because relaxing PoW's supply constraint implies a faster block rate which in turn increases disagreement among validators because blocks arrive too rapidly relative to network delay. A faster block rate paradoxically eventually increases wait times by prolonging the validator agreement process. This difficulty may be overcome only if the network consists of a single validator which eliminates the need for communication among validators. Thus, even allowing dynamic supply achieves widespread adoption only at the expense of decentralization.

The supply constraint can also be relaxed by increasing the number of transactions that can be recorded on any single block. Our model can be generalized to capture an alternative increase through larger block size. As noted by Decker and Wattenhofer (2013), the network delay increases linearly in the block size. Thus, a larger block size increases the fork propensity due to higher network delay and thereby also fails to remedy the limited adoption problem.

Proposition 4.5 may be interpreted as an economic parallel of Vitalik Buterin's Blockchain Trilemma.[10] Buterin's Trilemma pits decentralization, scalability and security against one another. Our analysis assumes security and demonstrates that a secure PoW payments blockchain cannot simultaneously achieve both scalability and decentralization. Proposition 4.3 demonstrates that a secure PoW payments blockchain cannot scale in the sense that such a blockchain cannot maintain a non-negligible market share when facing heightened demand. Proposition 4.5 then highlights that increasing the blockchain's throughput resolves the scalability issue only if that increased throughput induces centralization. Hence, a PoW payments blockchain cannot simultaneously achieve decentralization, scalability and security as Buterin suggested.

Proposition 4.6. *No Adoption Problem Without Network Delay*
Both widespread adoption (i.e., $\lim_{N\to\infty} c^* > 0$*) and decentralization (i.e.,* $\lim_{N\to\infty} V = \infty$*) can be obtained simultaneously under the counterfactual assumption of no network delay (i.e.,* $\Delta(V) = 0$*).*

Before transitioning to a discussion surrounding permissioned blockchains, we offer a final result to demonstrate the importance of network delay in generating our re-

[10]The interested reader may consult `https://github.com/ethereum/wiki/wiki/Sharding-FAQs` for further details.

sults. Proposition 4.6 assumes, counterfactually, that network delay does not exist (i.e., $\Delta(V) = 0$). Under this assumption a PoW payments blockchain can overcome the limited adoption problem. Widespread adoption becomes possible for a decentralized PoW system in the absence of network delay which establishes that network delay constitutes a critical factor for our results.

Our results highlight that limited adoption constitutes an endogenous and endemic characteristic of PoW payments blockchains. PoW combines an artificial supply constraint, free entry among validators and network delay that collectively make the system intrinsically impractical for widespread adoption (Proposition 4.3). Relaxing the supply constraint fails to overcome limited adoption for a decentralized PoW blockchain (Proposition 4.5). Our results do not argue against the potential for blockchain more broadly. In fact, we subsequently offer an alternative blockchain solution that overcomes the limited adoption problem.

5 A Permissioned Alternative

Proposition 4.5 highlights that a PoW payments blockchain must centralize to overcome the limited adoption problem. In this section, we consider a semi-centralized alternative: a permissioned blockchain.[11] Section 5.1 formally puts forth the permissioned blockchain model. Section 5.2 establishes that permissioned blockchains can obtain low confirmation times and widespread adoption.

Nonetheless, those benefits are insufficient for a blockchain to be viable. Establishing blockchain security constitutes a necessary condition for blockchain viability. We consider that topic for a permissioned blockchain in Sections 5.3 and 5.4. Section 5.3 introduces a standard consensus protocol and demonstrates that this protocol may in-

[11] Our focus upon permissioned blockchains does not imply that a permissionless setting cannot overcome the limited adoption problem. Some promising permissionless protocols include Byzantine Consensus PoS (e.g., Chen and Micali (2016)), delegated PoS (e.g., Kiayias et al. (2017)) and off-chain solutions (e.g., Poon and Dryja (2016) and Li, Wang, Xiei, and Zou (2019a)).

cur successful attacks in equilibrium. Section 5.4 introduces an alternative protocol that overcomes both the limited adoption problem and blockchain attacks.

5.1 Permissioned Blockchain Model

We model users as in Section 3 since the blockchain itself does not affect transaction demand. Unlike Section 3, we exogenously specify a set of validators, $V_P \in \mathbb{N}$.[12] All transactions enter at $t = 0$ at a single node so that all validators observe the full set of transactions by $t = \Delta(V_P)$. As with a PoW setting, validators instantly validate transactions. However, unlike a PoW setting, they need not solve any puzzle to partake in the consensus process so that no artificial supply constraint exists.

PoW attempts to create incentives for validators to not maliciously attack the blockchain. Thus, in offering an alternative, we focus on not only user adoption but also validator incentives. Validator i selects $a_i \in \{0,1\}$ with $a_i = 0$ corresponding to malicious behavior and $a_i = 1$ corresponding to honest behavior. Malicious behavior yields some profit, $\Pi > 0$, if the attack succeeds. In contrast, a failed attack imposes a cost, $\kappa > 0$, on a malicious validator. For simplicity, we assume that an honest validator earns neither a profit nor a loss. The success of an attack depends upon the blockchain's consensus protocol which we discuss later in this section.

A permissioned blockchain may possess a cryptocurrency which enables a blockchain designer to shape validator incentives. We invoke a cryptocurrency when designing our own consensus protocol and denote Validator i's holding of that cryptocurrency by $\alpha_i \in \mathbb{R}$.

We define a consensus protocol as a function $\omega : \{0,1\}^{V_P} \times \mathbb{R}^{V_P} \mapsto \{p \in [0,1]^{V_P} : \sum_{i=1}^{V_P} p_i = 1\}$ with ω_i corresponding to the probability that Validator i's ledger becomes the consensus ledger.[13] We further define $\Gamma(a_1, ..., a_{V_P}, \alpha_1, ..., \alpha_{V_P}) \equiv \sum_{i=1}^{V_P} \omega_i(a_1, ..., a_{V_P}, \alpha_1, ..., \alpha_{V_P})\, a_i$

[12] For exposition, we impose $V_P \geqslant 3$ in the equilibrium analysis.

[13] Our consensus protocol specification arises as a simplification of the more general construct.

so that Γ gives the probability that the blockchain does not suffer a successful attack.

Saleh (2019a) demonstrates that a cryptocurrency's price depends upon validator behavior on the associated blockchain. Taking such a premise as given, we assume that $P_{\Delta(V_P)} = P_H$ if the blockchain does not suffer a successful attack and $P_{\Delta(V_P)} = P_L$ otherwise with $P_t, t \in \{0, \Delta(V_P)\}$, denoting the time-$t$ cryptocurrency price and $P_H > P_L > 0$.

Definition 5.1. Permissioned Equilibrium

A Permissioned Equilibrium is an entrant cut-off, $c_P^* \in [0,1]$, a cryptocurrency price, P_0, a set of validator decisions, $\{a_i\}_{i=1}^{V_P} \in \{0,1\}^{V_P}$ and a set of validator cryptocurrency holdings, $\{\alpha_i\}_{i=1}^{V_P} \in \mathbb{R}^{V_P}$, given a validator network size, $V_P \geqslant 3$, a number of users, $N \geqslant 2$, a blockchain utility, $R_P > 0$, and a consensus protocol, ω, such that:

(i) $\forall i : c_i \leqslant c_P^* \Leftrightarrow R_P - c_i \Delta(V_P) \geqslant 0$

(ii) $(a_i, \alpha_i) \in \underset{(a,\alpha)}{\arg\sup}\ \Phi(a, \alpha; a_{-i}, \alpha_{-i})$
with $\Phi(a, \alpha; a_{-i}, \alpha_{-i}) \equiv (\Pi - (\Pi + \kappa)\mathbb{E}[\Gamma(a, a_{-i}, \alpha, \alpha_{-i})])\mathcal{I}_{a=0} + \alpha(\mathbb{E}[P_{\Delta(V_P)}] - P_0)$

(iii) $P_0 = \Gamma P_H + (1 - \Gamma) P_L$.

Definition 5.1 defines a Permissioned Equilibrium.[14] Definition 5.1 (i) asserts that a user employs the blockchain if and only if she (weakly) gains from employing the blockchain instead of a traditional payment system. Definition 5.1 (ii) requires that validators act optimally. We assume that all validators possess risk neutral preferences with perfect patience so that Definition 5.1 (iii) constitutes a necessary condition for equilibrium.

[14]For exposition, we restrict our attention to pure strategies.

5.2 Permissioned Blockchain Benefits

Proposition 5.1. *Lower Payment Confirmation Times*

For any PoW protocol, there exists a permissioned blockchain which induces (weakly) lower payment confirmation times.

Section 4 demonstrates that PoW suffers from large payment confirmation times. This issue arises due to an artificial supply constraint and network delay which can be exacerbated by the permissionless nature of a PoW blockchain. A permissioned blockchain that omits PoW's artificial supply constraint enables lower payment confirmation times. Proposition 5.1 formalizes that assertion.

Proposition 5.2. *No Limited Adoption Problem*

In any Permissioned Equilibrium, widespread adoption (i.e., $\lim_{N\to\infty} c_P^* = \min\{\frac{R_P}{\Delta(V_P)}, 1\} > 0$*) obtains.*

Section 4 establishes that PoW faces the limited adoption problem. Proposition 5.2 highlights that a permissioned blockchain does not face that problem. This result arises because the lack of an artificial supply constraint facilitates timely service even for high transaction volumes. Thus, as Proposition 5.2 posits, a permissioned blockchain may obtain widespread adoption.

5.3 Majority Rule Consensus

Definition 5.2. Majority Rule Permissioned Equilibrium (MRPE)

A Majority Rule Permissioned Equilibrium (MRPE) is a Permissioned Equilibrium such that voting power is equally distributed among the majority.[15] More formally, $\omega_i \equiv \mathcal{I}\{|S_{a_i}| > |S_{1-a_i}| \vee |S_{a_i}| = |S_{1-a_i}| \wedge a_i = 0\} \times \frac{1}{|S_{a_i}|}$. Moreover, $S_a \equiv \{i : a_i = a\}$.

Lemma 5.3. *Majority Rule Permissioned Equilibrium (MRPE)*

For a Majority Rule Permissioned Equilibrium (MRPE), the blockchain does not suffer a

[15] In case of a tie, we treat the malicious validators as the majority.

successful attack if and only if honest validators strictly outnumber malicious validators (i.e., $\Gamma = \mathcal{I}\{|S_1| > |S_0|\}$*).*

Definition 5.2 specializes Definition 5.1 to a standard permissioned blockchain protocol. This standard permissioned blockchain protocol determines blockchain updates by a simple majority rule. Lemma 5.3 formalizes that assertion.

As established by Proposition 5.2, a majority rule permissioned blockchain overcomes the limited adoption problem. Nonetheless, the viability of a blockchain requires also that it overcomes attacks. We discuss this issue subsequently.

Proposition 5.4. *Honest MRPE*
There exists an MRPE in which all validators behave honestly and the blockchain does not suffer a successful attack (i.e., $\exists$*MRPE s.t.* $\forall i : a_i = 1, \Gamma = 1$*).*

Proposition 5.4 establishes the existence of an equilibrium in which all validators behave honestly. This result arises because a single validator cannot successfully attack the blockchain by behaving maliciously if all other validators behave honestly. Malicious behavior yields a cost to reputation with no off-setting gain so that honest behavior constitutes the unique best response to all other validators behaving honestly.

Proposition 5.5. *Malicious MRPE*
There exists an MRPE in which all validators behave maliciously and the blockchain suffers a successful attack (i.e, $\exists$*MRPE s.t.* $\forall i : a_i = 0, \Gamma = 0$*).*

Proposition 5.5 establishes the existence of a second equilibrium in which all validators behave maliciously. This result arises because a single validator cannot unilaterally thwart a blockchain attack by behaving honestly. Honest behavior forgoes a reward from colluding to attack the blockchain when all other validators behave maliciously. Consequently, malicious behavior constitutes the unique best response to all other validators behaving maliciously.

Proposition 5.5 raises concern about employing a permissioned blockchain with a majority rule consensus protocol. Ideally, we wish a blockchain to both overcome the limited adoption problem and possess no equilibria in which a blockchain attack succeeds. Section 5.4 offers an alternative protocol that achieves both the desired goals.

5.4 Stake-Based Consensus

Definition 5.3. Stake-Based Permissioned Equilibrium (SBPE)
A Stake-Based Permissioned Equilibrium (SBPE) is a Permissioned Equilibrium such that voting power is equally distributed among the validators with majority stake.[16] More formally, $\omega_i \equiv \mathcal{I}\{T_{a_i} > T_{1-a_i} \vee T_{a_i} = T_{1-a_i} \wedge a_i = 0\} \times \frac{1}{|S_{a_i}|}$ with $T_a \equiv \sum_{i \in S_a} \alpha_i^+$.

Lemma 5.6. *Stake-Based Permissioned Equilibrium (SBPE)*
For a Stake-Based Permissioned Equilibrium (SBPE), the blockchain does not suffer a successful attack if and only if the cumulative stake of honest validators strictly outweighs that of malicious validators (i.e., $\Gamma = \mathcal{I}\{T_1 > T_0\}$).

Definition 5.3 specializes Definition 5.1 to a permissioned blockchain protocol that we refer to as a stake-based protocol. This protocol determines blockchain updates by majority stake (with zero weights given to short-sale positions) rather than majority rule. By majority stake we refer to a protocol under which a validators' vote is weighted by her holding in the native cryptocurrency. Lemma 5.6 formalizes that result.

Proposition 5.7. *Honest SBPE*
There exists an SBPE in which all validators behave honestly and the blockchain does not suffer a successful attack (i.e., $\exists$SBPE s.t. $\forall i : a_i = 1, \Gamma = 1$).

Proposition 5.7 establishes the existence of an equilibrium in which all validators behave honestly. This equilibrium arises for similar reasons as that described within Proposition 5.4, so we omit further discussion.

[16] In case of a tie, we treat the malicious validators as having the larger stake.

Proposition 5.8. *No Malicious SBPE*

There exists no SBPE in which an attack succeeds with strictly positive probability (*i.e.*, $\Gamma = 1$ *for all equilibria*).

Proposition 5.8 highlights the non-existence of an equilibrium in which a blockchain attack succeeds. This result arises because a single validator may become marginal by acquiring a sufficiently large stake. Since a validator's profit varies with her cryptocurrency position, she opts to become marginal and prevent a blockchain attack if she believes that an attack succeeds otherwise. Thus, a blockchain attack cannot succeed in equilibrium. A stake-based permissioned blockchain overcomes both blockchain attacks and the limited adoption problem.

6 Conclusion

Bitcoin has been envisioned as an alternative to traditional payment systems. While some vendors have adopted Bitcoin and other PoW payments platforms, no such platform has obtained widespread adoption. We demonstrate that this lack of widespread adoption constitutes an inescapable property of decentralized PoW payments blockchains. We consider permissioned blockchains as an alternative to PoW blockchains and demonstrate that permissioned blockchain may overcome the limited adoption problem.

This paper has important policy implications. It directly concerns adoption of blockchain as a payment system. The limited adoption problem makes PoW payments blockchains impractical for widespread adoption as a payment system. Our work highlights the need for research examining alternative protocols.

References

Abadi, J., and M. Brunnermeier. 2018. Blockchain Economics. *NBER Working Paper* .

Alsabah, H., and A. Capponi. 2019. Pitfalls of Bitcoin's Proof-of-Work: R&D Arms Race and Mining Centralization. *Working Paper* .

Basu, S., D. Easley, M. O'Hara, and E. Sirer. 2019. Towards a Functional Fee Market for Cryptocurrencies. *Working Paper* .

Biais, B., C. Bisière, M. Bouvard, and C. Casamatta. 2019. The Blockchain Folk Theorem. *Review of Financial Studies* 32:1662–1715.

Biais, B., C. Bisière, M. Bouvard, C. Casamatta, and A. J. Menkveld. 2018. Equilibrium Bitcoin Pricing. *Working Paper* .

Budish, E. 2018. The Economic Limits of Bitcoin and the Blockchain. *NBER Working Paper* .

Cao, S., L. W. Cong, and B. Yang. 2018. Auditing and Blockchains: Pricing, Misstatements, and Regulation. *Working Paper* .

Carlsten, M., H. Kalodner, S. M. Weinberg, and A. Narayanan. 2016. On the Instability of Bitcoin Without the Block Reward. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* pp. 154–167.

Catalini, C., and J. Gans. 2019. Initial Coin Offerings and the Value of Crypto Tokens. *NBER Working Paper* .

Chen, J., and S. Micali. 2016. ALGORAND: The Efficient and Democratic Ledger. *CoRR* abs/1607.01341. URL http://arxiv.org/abs/1607.01341.

Chiu, J., and T. V. Koeppl. 2017. The Economics of Cryptocurrencies - Bitcoin and Beyond. *Working Paper* .

Chiu, J., and T. V. Koeppl. 2019. Blockchain-based Settlement for Asset Trading. *Review of Financial Studies* Forthcoming.

Chod, J., and E. Lyandres. 2018. A Theory of ICOs: Diversification, Agency, and Information Asymmetry. *Working Paper* .

Chod, J., N. Trichakis, G. Tsoukalas, H. Aspegren, and M. Weber. 2018. Blockchain and The Value of Operational Transparency for Supply Chain Finance. *Working Paper* .

Chung, F., and L. Lu. 2002. The average distances in random graphs with given expected degrees. *Proceedings of the National Academy of Sciences* 99:15879–15882.

Cong, L. W., and Z. He. 2019. Blockchain Disruption and Smart Contracts. *Review of Financial Studies* 32:1754–1797.

Cong, L. W., Z. He, and J. Li. 2018. Decentralized mining in centralized pools. *Working Paper* .

Cong, L. W., Y. Li, and N. Wang. 2019a. Tokenomics and Platform Finance. *Working Paper* .

Cong, L. W., Y. Li, and N. Wang. 2019b. Tokenomics: Dynamic Adoption and Valuation. *Working Paper* .

Daian, P., R. Pass, and E. Shi. 2019. Snow White: Robustly Reconfigurable Consensus and Applications to Provably Secure Proof of Stake. Cryptology ePrint Archive, Report 2016/919. https://eprint.iacr.org/2016/919.

Davydiuk, T., D. Gupta, and S. Rosen. 2019. De-crypto-ing Signals in Initial Coin Offerings: Evidence of Rational Token Retention. *Working Paper* .

Decker, C., and R. Wattenhofer. 2013. Information Propagation in the Bitcoin Network. *IEEE P2P 2013 Proceedings* .

Easley, D., M. O'Hara, and S. Basu. 2019. From Mining to Markets: The Evolution of Bitcoin Transaction Fees. *Journal of Financial Economics* Forthcoming.

Eyal, I., and E. G. Sirer. 2014. Majority is not enough: Bitcoin mining is vulnerable. In *Eighteenth International Conference on Financial Cryptography and Data Security (FC'14)*.

Falk, B. H., and G. Tsoukalas. 2018. Token Weighted Crowdsourcing. *Working Paper* .

Fanti, G., L. Kogan, and P. Viswanath. 2019. Economics of Proof-of-Stake Payment Systems. *Working Paper* .

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

Foley, S., J. R. Karlsen, and T. J. Putnins. 2019. Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? *Review of Financial Studies* 32:1798–1853.

Gan, J., G. Tsoukalas, and S. Netessine. 2019. Inventory, Speculators, and Initial Coin Offerings. *Working Paper* .

Gandal, N., and H. Halaburda. 2016. Can we predict the winner in a market with network effects? Competition in the cryptocurrency market. *Games* 7.

Griffin, J. M., and A. Shams. 2018. Is Bitcoin Really Un-Tethered? *Working Paper* .

Gryglewicz, S., S. Mayer, and E. Morellec. 2019. Optimal Financing with Tokens. *Working Paper* .

Harvey, C. R. 2016. Cryptofinance. *Working Paper* .

Hinzen, F. J., F. Irresberger, K. John, and F. Saleh. 2019. The Public Blockchain Ecosystem: An Empirical Analysis. *NYU Stern Working Paper* .

Howell, S. T., M. Niessner, and D. Yermack. 2019. Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales. *Review of Financial Studies* .

Huberman, G., J. D. Leshno, and C. Moallemi. 2019. An Economic Analysis of the Bitcoin Payment System. *Working Paper* .

Jermann, U. 2018. Bitcoin and Cagan's Model of Hyperinflation. *Working Paper* .

Kiayias, A., A. Russell, B. David, and R. Oliynykov. 2017. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference*, pp. 357–388. Springer.

Kroeger, A., and A. Sarkar. 2017. The Law of One Bitcoin Price? *Working Paper* .

Lee, J., T. Li, and D. Shin. 2018. The Wisdom of Crowds in FinTech: Evidence from Initial Coin Offerings. *Working Paper* .

Li, J., and W. Mann. 2018. Initial Coin Offerings and Platform Building. *Working Paper* .

Li, J., K. Wang, J. Xiei, and D. Zou. 2019a. Crypto-Economics of the Nervos Common Knowledge Base. *Working Paper* .

Li, T., D. Shin, and B. Wang. 2019b. Cryptocurrency Pump-and-Dump Schemes. *Working Paper* .

Liu, Y., and A. Tsyvinski. 2018. Risks and Returns of Cryptocurrency. *NBER Working Paper* .

Liu, Y., A. Tsyvinski, and X. Wu. 2019. Common Risk Factors in Cryptocurrency. *NBER Working Paper* .

Makarov, I., and A. Schoar. 2019. Trading and Arbitrage in Cryptocurrency Markets. *Journal of Financial Economics* Forthcoming.

Malinova, K., and A. Park. 2018. Tokenomics: When Tokens Beat Equity. *Working Paper* .

Mayer, S. 2019. Token-Based Platforms and Speculators. *Working Paper* .

Miller, A., and J. J. LaViola. 2014. Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin. *http://nakamotoinstitute.org/research/anonymous-byzantine-consensus* .

Nayak, K., S. Kumar, A. Miller, and E. Shi. 2015. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack. Cryptology ePrint Archive, Report 2015/796. http://eprint.iacr.org/2015/796.

Pagnotta, E. 2018. Bitcoin as Decentralized Money: Prices, Mining Rewards, and Network Security. *Working Paper* .

Pagnotta, E., and A. Buraschi. 2018. An equilibrium valuation of bitcoin and decentralized network assets. *Working paper* .

Poon, J., and T. Dryja. 2016. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. *Working Paper* .

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

Riordan, O., and N. Wormald. 2010. The diameter of sparse random graphs. *Combinatorics, Probability and Computing* 19:835–926.

Rosu, I., and F. Saleh. 2019. Evolution of Shares in a Proof-of-Stake Cryptocurrency. *Working Paper* .

Saleh, F. 2019a. Blockchain Without Waste: Proof-of-Stake. *Working Paper* .

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

Shams, A. 2019. What Drives the Covariation of Cryptocurrency Returns? *Working Paper* .

Sockin, M., and W. Xiong. 2018. A model of cryptocurrencies. *Working Paper* .

Tinn, K. 2018. 'Smart' Contracts and External Financing. *Working Paper* .

Yermack, D. 2015. Is Bitcoin a Real Currency? An economic appraisal. *Handbook of Digital Currency* pp. 31–43.

Appendices

A CTMC Blockchain Model

We model the blockchain as a Continuous Time Markov Chain (CTMC), $\{X_t\}_{t\geqslant 0}$, with states $x \in X \equiv \{0, 1, ..., b\}$ with $x < b$ denoting that the blockchains last x heights contain single block and $x = b$ denoting the complement. Given the discussion in Section 3, $x < b$ corresponds to the blockchain being in the midst of a fork and $x = b$ corresponds to the complement. This section offers background results including the stationary distribution and sojourn times.

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 $p \equiv p(\Lambda, \Delta(V)) = 1 - e^{-\Lambda\Delta(V)} \in (0, 1)$. Then, $\forall x \in X/\{0, b\} : Q_{x,x} = -\Lambda$, $\forall x \in X/\{0\} : Q_{x,0} = \Lambda p$, $\forall x \in X/\{b\} : Q_{x,x+1} = \Lambda(1 - p)$, $Q_{b,b} = -\Lambda p$, $Q_{0,0} = -\Lambda(1 - p)$ and all other entries equal 0.

Lemma A.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 $\{N(t)\}_{t\geqslant 0}$ being a Poisson Process with rate λV.

Lemma A.2. *Fork Resolution 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 existence of a PoW equilibria.

Lemma A.3. *Monotone Fork Resolution Times*

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

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. $\forall x \in X/\{b\} : s_{x+1} \geqslant 0$ follows from $s_b = 0$. □

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

Lemma A.4. *Monotone Fork Resolution Derivatives*

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

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 $s_0 = e^{\Lambda\Delta(V)} + s_1$ so that $\frac{\partial s_0}{\partial \Lambda} > \frac{\partial s_1}{\partial \Lambda}$ follows immediately. Then, $s_x = 1 + e^{-\Lambda\Delta(V)}s_{x+1} +$

$(1-e^{-\Lambda\Delta(V)})s_0$ so that $\frac{\partial s_x}{\partial\Lambda} = e^{-\Lambda\Delta(V)}\frac{\partial s_{x+1}}{\partial\Lambda} + \Delta(V)e^{-\Lambda\Delta(V)}(s_0 - s_{x+1}) + (1-e^{-\Lambda\Delta(V)})\frac{\partial s_0}{\partial\Lambda} > \frac{\partial s_{x+1}}{\partial\Lambda}$ with the last inequality following by induction and Lemma A.3 which implies $\frac{\partial s_x}{\partial\Lambda} > \frac{\partial s_{x+1}}{\partial\Lambda}$ as desired. $\forall x \in X/\{b\} : \frac{\partial s_{x+1}}{\partial\Lambda} \geqslant 0$ follows from $\frac{\partial s_b}{\partial\Lambda} = 0$. Symmetry of the functions, $\{s_X\}_{x\in X}$, implies $\forall x \in X/\{b\} : \frac{\partial s_x}{\partial\Delta(V)} > \frac{\partial s_{x+1}}{\partial\Delta(V)} \geqslant 0$ which completes the proof. □

We 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 with parameter Λ and initial distribution $\{\pi_x\}_{x\in X}$. Then, by definition, $\tau = \tau(\Lambda, \Delta(V)) = \sum_{x\in X} \frac{s_x(\Lambda,\Delta(V))}{\Lambda}\pi_x(\Lambda, \Delta(V))$.

Lemma A.5. *Lower Bound for τ*

$\tau(\Lambda, \Delta(V)) \geqslant \Delta(V)\frac{e^{\Lambda\Delta(V)b}-1}{\Lambda\Delta(V)}$

Proof.

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

□

We define $\Psi(\Lambda, V) \equiv \tau(\Lambda, \Delta(V)) + \frac{1}{\Lambda}$ which equates with the expected wait time for the marginal user (i.e., Type $c_i = c^*$). Then, trivially, $\frac{\partial\Psi}{\partial V} = \frac{\partial\Psi}{\partial V}$.

Lemma A.6. *Increasing Wait Time in V*

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

Proof.

$$\begin{aligned}
&\Psi(\Lambda, V') - \Psi(\Lambda, V)\\
&= \tau(\Lambda, \Delta(V')) - \tau(\Lambda, \Delta(V))\\
&= \sum_{x\in X}\{\tfrac{s_x(\Lambda,\Delta(V'))}{\Lambda}\pi_x(\Lambda, \Delta(V')) - \tfrac{s_x(\Lambda,\Delta(V))}{\Lambda}\pi_x(\Lambda, \Delta(V))\}\\
&\geqslant \sum_{x\in X} \tfrac{s_x(\Lambda,\Delta(V'))-s_x(\Lambda,\Delta(V))}{\Lambda}\pi_x(\Lambda, \Delta(V))\\
&= \sum_{x\in X} \tfrac{1}{\Lambda}\int_V^{V'} \tfrac{\partial s_x}{\partial\Delta(V)}\Delta'(v)dv\ \pi_x(\Lambda, \Delta(V))\\
&> 0
\end{aligned}$$

□

Lemma A.7. *Zero Wait*

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

Proof.

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

B Proofs

Proposition 3.1 *Existence and Uniqueness of a PoW Equilibrium*

There exists a PoW Equilibrium. There exists no other equilibrium for which ϕ constitutes a strictly increasing and differentiable function on the interval $(0, c^*)$. The following conditions characterize the equilibrium:

(A) $\phi(c_i) = (N-1)\frac{c_i^2}{2\Lambda}$ *if* $c_i \leqslant c^*$ *and* $\phi(c_i) = 0$ *otherwise*

(B) $R < \Psi(\Lambda, \frac{(N-1)N}{6\beta\Lambda}) + \frac{N-1}{2\Lambda} \implies R = c^*\Psi(\Lambda, V) + \frac{(c^*)^2(N-1)}{2\Lambda}$

(C) $R \geqslant \Psi(\Lambda, \frac{(N-1)N}{6\beta\Lambda}) + \frac{N-1}{2\Lambda} \implies c^* = 1$

(D) $\beta V = (N-1)N\frac{(c^*)^3}{6\Lambda}$.

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. The interested reader may consult Appendix A for details. For exposition, we define $V^*(N, c^*, \Lambda, \beta) \equiv \frac{(N-1)N(c^*)^3}{6\beta\Lambda}$.

As a preliminary step, we rule out the existence of any equilibrium such that $c^* = 0$. By contradiction, we suppose there exists an equilibrium such that $c^* = 0$. Definition 3.1 (iv) implies $\max_{f \geqslant 0} R - c_i \cdot \mathbb{E}[W(f, f_{-i}) \mid c_i] - f \geqslant R - c_i \cdot \mathbb{E}[W(0, f_{-i}) \mid c_i] \geqslant R - c_i(\frac{N}{\Lambda} + \tau(\Lambda, V))$. Then, Definition 3.1 (ii) yields $\forall c_i > 0 : R - c_i(\frac{N}{\Lambda} + \tau(\Lambda, V)) \leqslant 0$ which in turn implies $R \leqslant 0$. $R \leqslant 0$ contradicts our assumption $R > 0$ and thereby eliminates the possibility of an equilibrium such that $c^* = 0$.

Problem 1 and Definitions 3.1 (iii) and (iv) yield $\max_{f \geqslant 0} R - c_i \cdot \mathbb{E}[W(f, f_{-i})|c_i] - f = \max_{f \geqslant 0} R - c_i \frac{(N-1)}{\Lambda} \mathbb{P}(\phi(c_j) \geqslant f \wedge c^* \geqslant c_j) - c_i \Psi(\Lambda, V) - f$. $\phi(c_i)$ being a strictly increasing function enables us to rewrite the latter problem as $\max_{f \geqslant 0} R - c_i \frac{(N-1)}{\Lambda} \max\{c^* - \phi^{-1}(f), 0\} - c_i \Psi(\Lambda, V) - f$. Differentiability of ϕ then yields $\frac{c_i(N-1)}{\Lambda} \frac{1}{\phi'(\phi^{-1}(f))} = 1$ as a first-order condition for $c_i \in (0, c^*)$. In equilibrium, $f_i = \phi(c_i)$ for $c_i \in [0, c^*]$ so that the latter condition simplifies to $\frac{c_i(N-1)}{\Lambda} = \phi'(c_i)$ for $c_i \in [0, c^*]$. In turn, that result implies $\phi(c_i) = (N-1)\frac{c_i^2}{2\Lambda}$ over $c \in [0, c^*]$. This result demonstrates that Proposition 3.1 (A) is necessary for the class of equilibria considered. Sufficiency for satisfying Definition 3.1 (i) follows from negativity of the objective's second derivative for Problem 1.

To establish existence and uniqueness of an equilibrium, we must establish the existence of some $V > 0$ and $c^* \in [0, 1]$ such that Definitions 3.1 (ii) and (v) hold with $\phi(c_i) = (N-1)\frac{c_i^2}{2\Lambda}$ given and Definitions 3.1 (iii) and (iv) taken as definitions for f_i and $W(f, f_i)$ respectively.

For $c^* \in (0, 1)$, Definition 3.1 (iii) and $\phi(c_i) = (N-1)\frac{c_i^2}{2\Lambda}$ imply Definition 3.1 (v) equates with $V^*(N, c^*, \Lambda, \beta) = V$. Moreover, 3.1 (ii) implies $\forall c_i > c^* : 0 > \max_{f \geqslant 0} R - c_i \cdot \mathbb{E}[W(f, f_{-i}) \mid c_i] - f \geqslant R - c_i \Psi(\Lambda, V) - \frac{(c^*)^2(N-1)}{2\Lambda}$ so that another application of 3.1 (ii) implies $R = c^* \Psi(\Lambda, V) + \frac{(c^*)^2(N-1)}{2\Lambda}$. Thus, existence and uniqueness equates with finding a unique solution, $c^* \in (0, 1)$, to $R = c^* \Psi(\Lambda, V^*(N, c^*, \Lambda, \beta)) + \frac{(c^*)^2(N-1)}{2\Lambda} \equiv G(c^*; N, \Lambda, \beta)$. Lemma A.7 yields $G(0; N, \Lambda, \beta) = 0 < R$ so that if $G(1; N, \Lambda, \beta) = \Psi(\Lambda, \frac{(N-1)N}{6\beta\Lambda}) + \frac{N-1}{2\Lambda} > R$ then continuity and strict monotonicity of G in c^* imply existence and uniqueness of an equilibrium with $c^* \in (0, 1)$ and $V = V^*(N, c^*, \Lambda, \beta)$.

To conclude, we need demonstrate only non-existence of an equilibrium with $c^* = 1$ if $\Psi(\Lambda, \frac{(N-1)N}{6\beta\Lambda}) + \frac{N-1}{2\Lambda} > R$ and existence of a unique equilibrium with $c^* = 1$ otherwise. If $c^* = 1$ then $V = \frac{(N-1)N}{6\beta\Lambda}$ uniquely satisfies Definition 3.1 (v) so that $R \geqslant \Psi(\Lambda, \frac{(N-1)N}{6\beta\Lambda}) + \frac{N-1}{2\Lambda}$ by Definitions 3.1 (ii) - (iv) and $\phi(c_i) = (N-1)\frac{c_i^2}{2\Lambda}$. Thus, no equilibrium with

$c^* = 1$ exists if $R < \Psi(\Lambda, \frac{(N-1)N}{6\beta\Lambda}) + \frac{N-1}{2\Lambda}$. Existence of a unique equilibrium with $c^* = 1$ follows because $c^* = 1$ and $V = \frac{(N-1)N}{6\beta\Lambda}$ satisfy all conditions for Definition 3.1 and all other choices for V violate Definition 3.1 (v).

□

Proposition 4.1 *Payment Confirmation Lower Bound*

Network delay bounds below all user payment confirmation times (i.e., $\forall i : W_i \geqslant \tau(\Lambda, V) \geqslant \Delta(V)$).

Proof.

Follows immediately from Lemma A.5 □

Lemma B.1. *Increasing V*

V increases in N and $\lim_{N\to\infty} V(N) = \infty$

Proof.

If $R \geqslant \Psi(\Lambda, \frac{(N-1)N}{6\beta\Lambda}) + \frac{N-1}{2\Lambda}$ then $\frac{dV}{dN} > 0$ follows from Proposition 3.1 (D). Otherwise, Proposition 3.1 (B) and (D) imply $R = \sqrt[3]{\frac{6\beta\Lambda V}{N(N-1)}}\Psi(\Lambda, V) + \sqrt[3]{\frac{9\beta^2 V^2(N-1)}{2\Lambda N^2}} \equiv H(V, N; \beta, \Lambda) \equiv H(V, N)$. Proposition 3.1 implies the existence of a non-negative function $V(N)$ that uniquely satisfies $R = H(V(N), N)$. By the implicit function theorem, $\frac{dV}{dN} = -\frac{\frac{\partial H}{\partial N}}{\frac{\partial H}{\partial V}} > 0$ which in turn implies the existence of $\lim_{N\to\infty} V(N)$. $0 \leqslant \lim_{N\to\infty} V(N) < \infty$ implies $\lim_{N\to\infty} H(V, N) = 0$ so that $\lim_{N\to\infty} H(V, N) = R > 0$ yields the desired conclusion. □

Proposition 4.2 *Arbitrarily Large Payment Confirmation Time*

All user payment confirmation times diverge as demand diverges, (i.e., $\forall i : \lim_{N\to\infty} W_i = \infty$). This result holds in particular for the marginal user (i.e., i such that $c_i = c^*$), who is serviced with highest priority (i.e., $\forall j : f_i \geqslant f_j$).

Proof.

Proposition 4.1 yields $W_i \geqslant \Psi(\Lambda, V) \geqslant \tau(\Lambda, V) \geqslant \Delta(V)$ so that Lemma B.1 and

$\lim_{V\to\infty} \Delta(V) = \infty$ delivers the result. □

Proposition 4.3 *An Adoption Problem*

Adoption decreases as demand rises (i.e., c^* decreases in N). Moreover, the blockchain faces limited adoption (i.e., $\lim_{N\to\infty} c^* = 0$).

Proof.

Proposition 3.1 and Lemma B.1 imply that c^* decreases in N so that $\lim_{N\to\infty} c^* \in [0,1]$ exists. $\lim_{N\to\infty} c^* \in (0,1]$ implies $\lim_{N\to\infty}\{c^*\Psi(\Lambda,V)+\frac{(c^*)^2(N-1)}{2\Lambda}\} = \infty$ so that $\lim_{N\to\infty}\{c^*\Psi(\Lambda,V)+\frac{(c^*)^2(N-1)}{2\Lambda}\} = R < \infty$ via Proposition 3.1 (B) yields $\lim_{N\to\infty} c^* = 0$ as desired. □

Proposition 4.4 *Endogenous Network Delay*

Let c_v^* denote the adoption rate of a network with variable network delay that satisfies the regularity discussed within Section 3. Let c_c^* denote the adoption rate of a network with constant network delay. Then, $c_v^* < c_c^*$ for large transaction demands (i.e., $\exists \underline{N} : \forall N > \underline{N} : c_v^* < c_c^*$).

Proof.

From Appendix A, recall that $\Psi(\Lambda,V) \equiv \tau(\Lambda,\Delta(V)) + \frac{1}{\Lambda}$. Let Δ_c denote the constant network delay (associated with c_c^*) and $\Delta_v(V)$ denote the variable network delay (associated with c_v^*). Then, Proposition 3.1 implies that $\forall N > 2R\Lambda+1 : c_v^*(\tau(\Lambda,\Delta_v(V))+\frac{1}{\Lambda}) + \frac{(c_v^*)^2(N-1)}{2\Lambda} = c_c^*(\tau(\Lambda,\Delta_c)+\frac{1}{\Lambda}) + \frac{(c_c^*)^2(N-1)}{2\Lambda}$. Lemmas A.5 and B.1 imply $\exists N_1 > 0 : \forall N \geqslant N_1 : \tau(\Lambda,\Delta_v(V)) \geqslant \tau(\Lambda,\Delta_c)$ so that $\forall N > \max\{N_1, 2R\Lambda+1\} \equiv \underline{N} : c_v^*(\tau(\Lambda,\Delta_c)+\frac{1}{\Lambda}) + \frac{(c_v^*)^2(N-1)}{2\Lambda} \leqslant c_c^*(\tau(\Lambda,\Delta_c)+\frac{1}{\Lambda}) + \frac{(c_c^*)^2(N-1)}{2\Lambda}$ which implies $\forall N > \underline{N} : c_v^* < c_c^*$ as desired. □

Proposition 4.5 *Decentralization implies Limited Adoption*

For exposition, we assume that $\lim_{N\to\infty} c^*$ exist. The blockchain necessarily faces either centralization (i.e., $\limsup_{N\to\infty} V \leqslant 1$) or limited adoption (i.e., $\lim_{N\to\infty} c^* = 0$).

Proof.

Formally, we consider a sequence of parameters $\{(N_n, \Lambda_n, R, \beta)\}_{n\in\mathbb{N}}$ with $R, \beta > 0$, $2 \leqslant N_n \nearrow \infty$. Then, following Proposition 3.1, there exists a sequence $\{(c_n^*, V_n)\}_{n\in\mathbb{N}}$ such that (c_n^*, V_n) corresponds to the equilibrium solution for a model with parameters $(N_n, \Lambda_n, R, \beta)$.

We proceed by contradiction. We assume that $L \equiv \limsup_{n\to\infty} V_n > 1$ and $M \equiv \lim_{n\to\infty} c_n^* > 0$. We take a subsequence, $\{(N_{n_j}, \Lambda_{n_j}, c_{n_j}^*, V_{n_j})\}_{j\in\mathbb{N}}$, such that $\forall j : V_{n_j} \geqslant \frac{1+L}{2}$. Then, Proposition 3.1 (B) and (C) yield $\Lambda_{n_j} \geqslant \frac{(c_{n_j}^*)^2(N_{n_j}-1)}{2R}$ so that $\lim_{j\to\infty} \Lambda_{n_j} = \infty$. Lemma A.5 and Proposition 3.1 (B) - (C) then give $R \geqslant c_{n_j}^* \Delta(V_{n_j}) \frac{e^{\Lambda_{n_j}\Delta(V_{n_j})}-1}{\Lambda_{n_j}\Delta(V_{n_j})}$ so that monotonicity of Δ coupled with $\forall j : V_{n_j} \geqslant \frac{1+L}{2}$ yields $R \geqslant c_{n_j}^* \Delta(\frac{1+L}{2}) \frac{e^{\Lambda_{n_j}\Delta(\frac{1+L}{2})}-1}{\Lambda_{n_j}\Delta(\frac{1+L}{2})}$. Finally, invoking $\lim_{j\to\infty} \Lambda_{n_j} = \infty$ gives $R \geqslant \lim_{j\to\infty} c_{n_j}^* \Delta(\frac{1+L}{2}) \frac{e^{\Lambda_{n_j}\Delta(\frac{1+L}{2})}-1}{\Lambda_{n_j}\Delta(\frac{1+L}{2})} = \infty$ delivering the desired contradiction and thereby completing the proof. □

Proposition 4.6 *No Adoption Problem Without Network Delay*

Both widespread adoption (i.e., $\lim_{N\to\infty} c^* > 0$) and decentralization (i.e., $\lim_{N\to\infty} V = \infty$) can be obtained simultaneously under the counterfactual assumption of no network delay (i.e., $\Delta(V) = 0$).

Proof.

Formally, we take a sequence of parameters $\{(N_n, R, \beta)\}_{n\in\mathbb{N}}$ such that $R, \beta > 0$, $2 \leqslant N_n \nearrow \infty$ and construct a sequence $\{\Lambda_n\}_{n=1}^{\infty}$. Then, we provide a sequence $\{(c_n^*, V_n)\}_{n\in\mathbb{N}}$ such that (c_n^*, V_n) corresponds to equilibrium solutions for a model with parameters $(N_n, \Lambda_n, R, \beta)$. We demonstrate that, given our choice, $\{\Lambda_n\}_{n=1}^{\infty}$, $\lim_{n\to\infty} c_n^* > 0$ and $\lim_{n\to\infty} V_n = \infty$ if $\Delta(V) = 0$ (i.e., no network delay). Note that this result does not contradict Proposition 4.5 as all parts of the paper (except this proposition) preclude $\Delta(V) = 0$ (i.e., we assume existence of network delay outside of this proposition).

Let $\Lambda_n \equiv \frac{N_n-1}{2}$. Let $c_n^* \equiv \min\{c_n, 1\}$ with c_n being the unique positive solution for $R = \frac{c_n}{\Lambda_n} + c_n^2$ and let $V_n = \frac{N_n(c^*)^3}{3}$. Then, $\{(c_n^*, V_n)\}_{n\in\mathbb{N}}$ satisfies all conditions from Definition 3.1 thereby constituting an equilibrium for $\{(N_n, R, \beta)\}_{n\in\mathbb{N}}$. Moreover, $\lim_{n\to\infty} c_n^* = c^* = \min\{\sqrt{R}, 1\} > 0$ and $\lim_{n\to\infty} V_n = \infty$ as desired. □

Proposition 5.1 *Lower Payment Confirmation Times*

For any PoW protocol, there exists a permissioned blockchain which induces (weakly) lower payment confirmation time.

Proof.

Let $V_P = V$. Then, the result follows from Proposition 4.1. □

Proposition 5.2 *No Limited Adoption Problem*

In any Permissioned Equilibrium, widespread adoption (i.e., $\lim_{N\to\infty} c_P^* = \min\{\frac{R_P}{\Delta(V_P)}, 1\} > 0$) obtains.

Proof.

$R_P - c_i\Delta(V_P)$ decreases in c_i so that Definition 5.1 (i) implies $c_P^* = \min\{\frac{R_P}{\Delta(V_P)}, 1\}$ so that $\lim_{N\to\infty} c_P^* = \min\{\frac{R_P}{\Delta(V_P)}, 1\}$ follows trivially. □

Lemma 5.3 *Majority Rule Permissioned Blockchain Equilibrium (MRPBE)*

For a Majority Rule Permissioned Equilibrium (MRPE), the blockchain does not suffer a successful attack if and only if honest validators strictly outnumber malicious validators (i.e., $\Gamma = \mathcal{I}\{|S_1| > |S_0|\}$).

Proof.

$\Gamma(x) = \sum_{i=1}^{V_P} \omega_i(x) a_i = \sum_{i\in S_1} \omega_i(x) = \mathcal{I}(|S(1)| > |S(0)|)$ □

Proposition 5.4 *Honest MRPBE*

There exists an MRPE in which all validators behave honestly and the blockchain does not suffer a successful attack (i.e., $\exists$MRPE s.t. $\forall i : a_i = 1, \Gamma = 1$).

Proof.

We demonstrate the existence of a symmetric equilibrium in which $c_P^* = \min\{1, \frac{R_P}{\Delta(V_P)}\}$,

$P_0 = P_H$ and $\forall i : (a_i, \alpha_i) = (1, 0)$. In such an equilibrium, all validators behave honestly since $\forall i : a_i = 1$ and $\Gamma = 1$ so that the blockchain does not sustain a successful attack.

Direct verification shows that $c_P^* = \min\{1, \frac{R_P}{\Delta(V_P)}\}$ satisfies Definition 5.1 (i) and $P_0 = P_H$ satisfies Definition 5.1 (iii). As such, to prove the result, we need only demonstrate that $\forall a \in \{0, 1\}, \alpha \in \mathbb{R} : \Phi(1, 0; a_{-i}, \alpha_{-i}) \geqslant \Phi(a, \alpha, a_{-i}, \alpha_{-i})$ with $\forall j \neq i : (a_j, \alpha_j) = (1, 0)$. $V_P \geqslant 3$ implies $\Gamma = 1$ so that $a \in \{0, 1\}, \alpha \in \mathbb{R} : \Phi(a, \alpha; a_{-i}, \alpha_{-i}) = -\kappa \mathcal{I}_{a=0} \leqslant 0 = \Phi(1, 0; a_{-i}, \alpha_{-i})$ as desired. □

Proposition 5.5 *Malicious MRPBE*

There exists an MRPE in which all validators behave maliciously and the blockchain suffers a successful attack (i.e, ∃MRPE s.t. $\forall i : a_i = 0, \Gamma = 0$*).*

Proof.

We demonstrate the existence of a symmetric equilibrium in which $c_P^* = \min\{1, \frac{R_P}{\Delta(V_P)}\}$, $P_0 = P_L$ and $\forall i : (a_i, \alpha_i) = (0, 0)$. In such an equilibrium, all validators behave maliciously since $\forall i : a_i = 0$ and $\Gamma = 0$ so that the blockchain sustains a successful attack with probability 1.

Direct verification shows that $c_P^* = \min\{1, \frac{R_P}{\Delta(V_P)}\}$ satisfies Definition 5.1 (i) and $P_0 = P_L$ satisfies Definition 5.1 (iii). As such, to prove the result, we need only demonstrate that $\forall a \in \{0, 1\}, \alpha \in \mathbb{R} : \Phi(0, 0; a_{-i}, \alpha_{-i}) \geqslant \Phi(a, \alpha, a_{-i}, \alpha_{-i})$ with $\forall j \neq i : (a_j, \alpha_j) = (0, 0)$. $V_P \geqslant 3$ implies $\Gamma = 0$ so that $a \in \{0, 1\}, \alpha \in \mathbb{R} : \Phi(a, \alpha; a_{-i}, \alpha_{-i}) = \Pi \mathcal{I}_{a=0} \leqslant \Pi = \Phi(0, 0; a_{-i}, \alpha_{-i})$ as desired. □

Lemma 5.6 *Stake-Based Permissioned Equilibrium (SBPE)*

For a Stake-Based Permissioned Equilibrium (SBPE), the blockchain does not suffer a successful attack if and only if the cumulative stake of honest validators strictly outweighs that of malicious validators (i.e., $\Gamma = \mathcal{I}\{T_1 > T_0\}$*).*

Proof.

$$\Gamma(x) = \sum_{i=1}^{V_P} \omega_i(x) a_i = \sum_{i \in S_1} \omega_i(x) = \mathcal{I}(\sum_{i \in S_1} \alpha_i^+ > \sum_{i \in S_0} \alpha_i^+) \qquad \square$$

Proposition 5.7 *Honest SBPE*

There exists an SBPE in which all validators behave honestly and the blockchain does not suffer a successful attack (i.e., $\exists$SBPE s.t. $\forall i : a_i = 1, \Gamma = 1$).

Proof.

We demonstrate the existence of a symmetric equilibrium in which $c_P^* = \min\{1, \frac{R_P}{\Delta(V_P)}\}$, $P_0 = P_H$ and $\forall i : (a_i, \alpha_i) = (1, \frac{\Pi}{P_H - P_L})$. In such an equilibrium, all validators behave honestly since $\forall i : a_i = 1$ and $\Gamma = 1$ so that the blockchain does not sustain a successful attack.

Direct verification shows that $c_P^* = \min\{1, \frac{R_P}{\Delta(V_P)}\}$ satisfies Definition 5.1 (i), and $P_0 = P_H$ satisfies Definition 5.1 (iii). As such, to prove the result, we need only demonstrate that $\forall a \in \{0,1\}, \alpha \in \mathbb{R} : \Phi(1, \frac{\Pi}{P_H - P_L}; a_{-i}, \alpha_{-i}) \geqslant \Phi(a, \alpha, a_{-i}, \alpha_{-i})$ with $\forall j \neq i : (a_j, \alpha_j) = (1, \frac{\Pi}{P_H - P_L})$. We define $\underline{\alpha} \equiv \frac{\Pi(V_P - 1)}{P_H - P_L} \geqslant \frac{2\Pi}{P_H - P_L} > 0$.

Then, $\forall a \in \{0,1\}, \alpha \in \mathbb{R}$:

$$\Phi(a, \alpha; a_{-i}, \alpha_{-i})$$

$$\leqslant \max\{ \sup_{\alpha^* < \underline{\alpha}} \Phi(a, \alpha^*; a_{-i}, \alpha_{-i}), \sup_{\alpha^* \geqslant \underline{\alpha}} \Phi(a, \alpha^*; a_{-i}, \alpha_{-i}) \}$$

$$\leqslant \max\{-\kappa \mathcal{I}_{a=0}, \max\{0, \Pi + (P_L - P_H)\underline{\alpha} \} \}$$

$$\leqslant 0$$

$\Phi(1, \frac{\Pi}{P_H - P_L}; a_{-i}, \alpha_{-i}) = 0$ completes the proof. $\square$

Proposition 5.8 *No Malicious SBPE*

There exists no SBPE in which an attack succeeds with strictly positive probability (i.e., $\Gamma = 1$ for all equilibria).

Proof.

We proceed by contradiction. We assume that there exists an equilibrium in which an attack succeeds with strictly positive probability (i.e., $\Gamma < 1$). Via Lemma 5.6, $\Gamma < 1 \implies \Gamma = 0$ which in turn implies $P_0 = P_L$ via Definition 5.1 (iii). Then, defining $\alpha_* \equiv \sum_{j \in S_0, j \neq 1} \alpha_j - \sum_{j \in S_1, j \neq 1} \alpha_j + 1$ implies $\sup_{(a,\alpha)} \Phi(a, \alpha; a_{-1}, \alpha_{-1}) \geqslant \sup_{\alpha \geqslant \alpha_*} \Phi(1, \alpha; a_{-1}, \alpha_{-1}) = \sup_{\alpha \geqslant \alpha_*} \alpha(P_H - P_0)$ so that $P_0 \geqslant P_H$ constitutes a necessary condition for equilibrium. $P_H > P_L = P_0 \geqslant P_H$ gives the desired contradiction thereby completing the proof. □