Proof-of-Work's Limited Adoption Problem[*]

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

February 12, 2019

Abstract

We demonstrate that a limited adoption problem arises endogenously in a Proof-of-Work (PoW) payments blockchain. Increased transaction demand increases fees because PoW imposes an artificial supply constraint. The increased fees in turn induce validators to enter the network because of PoW's permissionless nature. The increased network size protracts the consensus process and thereby delays payment confirmation. Given access to traditional payment systems, users prefer to transact via the blockchain only if they possess extreme insensitivity to delays. A PoW payments blockchain therefore cannot obtain widespread adoption. A permissioned blockchain offers an alternative to overcome this problem because such a blockchain neither imposes PoW's artificial supply constraint nor admits free entry among validators. Nonetheless, validators may collude on such a blockchain if implemented with a standard consensus protocol. We offer an alternative consensus protocol that overcomes such collusion. Our protocol employs the blockchain's native cryptocurrency to induce the desired behavior and thereby provides both expedient transaction processing and blockchain security.

Keywords: Blockchain, Proof-of-Work, Limited Adoption, FinTech, Stake

JEL Classification: E50, G12

[*] We thank William Cong, Gur Huberman and Ari Juels 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 regarding whether Bitcoin's limited usage arises due to its infancy 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 PoW payments blockchains make limited adoption an inescapable equilibrium outcome. Our critique does not apply to other blockchains such as smart contract platforms and permissioned platforms. As such, our work highlights the need for research on alternatives in the nascent field of blockchain economics.

PoW dates back to Dwork and Naor (1992) and later gained mainstream attention when Nakamoto (2008) popularized the concept by employing it to allegedly induce good validator behavior within a permissionless blockchain setting.[1,2] Nakamoto (2008) envisioned a decentralized network that admits free entry and perfect competition among validators. To achieve that vision while creating appropriate validator incentives, Nakamoto (2008) specified that agents must solve a verifiable puzzle to update the blockchain.[3] Nakamoto (2008) specified the puzzle difficulty as a parameter so that the block arrival rate (i.e., rate of blockchain updating) may be targeted. The motivation for this targeting feature arises from the premise that blockchain updates occurring faster than network latency undermines validators agreeing on ledger contents.[4] Narayanan, Bonneau, Felten, Miller, and Goldfeder (2016) argue that the block rate "should be [targeted as] a fixed amount" because "blocks [coming] very close together [induces] a lot of inefficiency" due to "latency." The block arrival rate targeting, however, artificially constrains ledger space. We demonstrate that this artificial sup-

[1] Validators on a Proof-of-Work blockchain are called miners.

[2] A permissionless blockchain constitutes a blockchain that admits free entry with respect to the validator network.

[3] The interested reader may consult Biais, Bisière, Bouvard, and Casamatta (2019) for further reference.

[4] Network latency references the time required for information to travel across the network.

ply constraint interacts with network latency and PoW's permissionless nature to make limited adoption endemic to PoW payments blockchains.

Due to PoW's supply constraint, an increase in transaction demand endogenously generates an increase in fees. That fee increase in turn induces validators to enter the PoW network. The PoW network expansion then exacerbates network latency and protracts the validator agreement process. For users, this delay amounts to increased payment confirmation times which drives users away from the blockchain platform towards traditional payment systems. In equilibrium, the blockchain maintains only users relatively insensitive to payment confirmation delays. Thus, our analysis demonstrates that PoW payments blockchains cannot simultaneously sustain large volumes and a non-negligible payments market share - we term this problem the Limited Adoption Problem.

To overcome the Limited Adoption Problem, we consider dynamic adjustment of PoW's block rate. We find that such an adjustment succeeds only if the blockchain becomes centralized. If the block rate fails to keep pace with transaction demand, prohibitive wait times drive users from the blockchain. Alternatively, if the block rate keeps pace with transaction demand, a protracted validator agreement process drives users away from the blockchain. This reasoning breaks down only if the PoW blockchain features just one validator. A single validator network allows simultaneously for arbitrarily large block rates and an expedient validator agreement process.

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 a permissioned blockchain.

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 reputational cost from unsuccessfully attacking the blockchain. 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.

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), Biais, Bisière, Bouvard, and Casamatta (2019) and Cong, He, and Li (2018) analyze PoW mining strategies. Huberman, Leshno, and Moallemi (2018) 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. Kroeger and Sarkar (2017), Biais, Bisière, Bouvard, Casamatta, and Menkveld (2018), Hinzen (2018), Li, Shin, and Wang (2018), Liu and Tsyvinski (2018), Makarov and Schoar (2018) and Pagnotta and Buraschi (2018) study the determinants of cryptoasset prices. Other notable works include Gandal and Halaburda (2016), Harvey (2016), Abadi and Brunnermeier (2018), Griffin and Shams (2018) and Jermann (2018).

This paper highlights an important shortcoming of PoW payments blockhains. 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 (2018) theoretically demonstrate that PoW contributes to that price volatility; Saleh (2018) 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. 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. Cong, Li, and Wang (2018), Sockin and Xiong (2018), Cong and He (2019) and Cong, Li, and Wang (2019) depart from the Bitcoin paradigm by examining a blockchain platform that possesses functionality beyond payment processing. Falk and Tsoukalas (2018) provide theoretical analysis of blockchain-based token weighted voting platforms. Chod and Lyandres (2018), Lee, Li, and Shin (2018), Li and Mann (2018), Malinova and Park (2018), Niessner, Howell, and Yermack (2018) and Catalini and Gans (2019) study initial coin offerings. Basu, Easley, O'Hara, and Sirer (2019) propose an alternative fee setting mechanism to that employed by Bitcoin. Saleh (2019) formally analyzes Proof-of-Stake (PoS) and establishes that such a protocol induces consensus under certain conditions.

Also notable, there exists a large literature within computer science that studies security of various blockchain protocols. Some papers within that literature include Miller and LaViola (2014), Gilad, Hemo, Micali, Vlachos, and Zeldovich (2017), Kiayias, Russell, David, and Oliynykov (2017) and Daian, Pass, and Shi (2019). Our paper differs from those works in that those papers rely upon some exogenous behavioral assumptions whereas our paper conducts a full equilibrium analysis. Our paper omits an exogenously-motivated attacker and therefore does not analyze security in the same sense as the computer science literature.

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

2 PoW Model

We model an infinite horizon 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.

2.1 Users

Our model involves finitely many users, $i \in \{1, ..., N\}$. At $t = 0$, User i learns her type, $c_i \sim U[0,1]$, which remains unknown to others.[5] We model user preferences akin to Huberman, Leshno, and Moallemi (2018) with each user possessing only one transaction and c_i denoting the delay cost for User i.

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

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

After learning her type, User i selects a fee level, f_i, that solves Problem 1. $W(f_i, f_{-i})$ represents the time that User i's transaction earns confirmation whereas R represents the utility of User i having her transaction processed. If $\max_{f_i \geqslant 0} R - c_i \cdot \mathbb{E}[W(f_i, f_{-i})|c_i] - f_i < 0$ then User i opts to transact via traditional payment systems rather than on the blockchain.

2.2 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 computer, and we assume that each computer possesses identical hashing power so that each validator expects to earn an equal share of fees. We assume validators possess risk-neutral preferences. Then, free entry yields Equation 2 with V being the equilibrium number of validators and T corresponding to the set of users who transact on the blockchain.

$$V = \frac{\mathbb{E}[\sum\limits_{i \in T} f_i]}{\beta} \tag{2}$$

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

2.3 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 latency 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 mining 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 latency 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]

We assume that payments cannot be confirmed during a fork because, in such a case, validators disagree regarding the ledger's contents. Once a fork arises, we require a "k-blocks" rule to resolve the fork. Specifically, we require k consecutive arrivals without multiple blocks at the same height to return the blockchain to consensus.

2.4 Equilibrium

Definition 2.1. PoW Equilibrium

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

(i) $\forall i : f(c_i)$ solves Problem 1 with $f(0) = 0$ for $c_i \leqslant c^*$

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

[6] $\Delta(V)$ 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.

(iii) $W(f_i, f_{-i}) = \sum\limits_{j \neq i : f_i \leqslant f_j} H_j + Z_i, H_j \sim exp(\Lambda), \mathbb{E}[Z_i] = \Psi(\Lambda, V)$.[7]

(iv) $\beta V = \mathbb{E}[\sum\limits_{i \in T} f(c_i)]$ with $T \equiv \{i : c_i \leqslant c^*\}$.

Definition 2.1 defines 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. Definition 2.1 (i) asserts that users select an optimal fee schedule. Definition 2.1 (ii) states that a user transacts on the blockchain if and only if she (weakly) gains utility from transacting on the blockchain relative to traditional payment systems. Definition 2.1 (iii) characterizes wait times as decoupling into the wait for higher priority transactions and the wait for fork resolution. Definition 2.1 (iv) imposes no profits for validators in equilibrium because free entry characterizes the validator network.

Proposition 2.1. *Existence and Uniqueness of a PoW Equilibrium*
There exists a PoW Equilibrium. There exists no other equilibrium for which f constitutes a strictly increasing and differentiable function. The following conditions characterize the equilibrium:

(A) $f(c_i) = (N-1)\frac{c_i^2}{2\Lambda}$

(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 2.1 establishes existence and uniqueness of a PoW Equilibrium. This result ensures coherence of the subsequent discussion.

[7] $\Psi(\Lambda, V) \equiv \mathbb{E}[W(f_i, f_{-i}) \mid c_i = c^*]$. For more detail we refer the interested reader to Appendix A.

3 PoW Results

Having established existence and uniqueness of a PoW Equilibrium, we turn to analyzing the properties of that equilibrium. Section 3.1 analyzes payment confirmation times. Section 3.2 establishes the Limited Adoption Problem and related results.

3.1 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] $(N-1)\frac{(c^* - c_i)}{\Lambda}$ refers to the expected service time for higher priority users. $\frac{1}{\Lambda}$ equals the expected service time for User i. $\tau(\Lambda, V)$ denotes the expected fork resolution time.[9]

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

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 3.1. *Payment Confirmation Lower Bound*

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

[8] Equation 3 follows from Definition 2.1 (iii) and Proposition 2.1 (A)

[9] The interested reader may consult Appendix A for further detail regarding $\tau(\Lambda, V)$.

Proposition 3.1 asserts that PoW induces a strictly positive 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 3.2. *Arbitrarily Large Marginal Payment Confirmation Time*
All user payment confirmation times diverge as demand diverges ($i.e., \forall i: \lim\limits_{N \to \infty} W_i = \infty$). *This result holds in particular for the highest priority user, i.e., i such that $c_i = c^*$.*

Next, we turn our attention to how payment confirmation times vary with increases in transaction demand. Proposition 3.2 asserts that payment confirmation times diverge for all users, including the highest priority user, as transaction demand grows.[10]

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 latency 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.

3.2 Limited Adoption Problem

The aforementioned elongated payment confirmation times have important implications regarding the viability of a PoW payments blockchain. Specifically, a PoW payments blockchain cannot simultaneously sustain a large volume and a non-negligible market share. Proposition 3.3 formalizes that result which we term the Limited Adoption Problem.

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

Proposition 3.3. *Limited Adoption Problem*

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

Section 3.1 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.[11]

One may conjecture that a relaxation of PoW's artificial supply constraint (i.e., increasing Λ) solves the Limited Adoption Problem. Proposition 3.4, however, demonstrates that such an approach succeeds only in so far as it induces centralization. This result arises because relaxing PoW's artificial supply constraint implies a faster block rate which in turn increases disagreement among validators because blocks arrive too rapidly relative to network latency. A faster block rate paradoxically eventually increases wait times by prolonging the validator agreement process. This difficulty may be overcome only if the network possesses one validator which eliminates the need for communication among validators. Thus, even allowing dynamic supply achieves widespread adoption only at the expense of decentralization. The notion of sacrificing decentralization to obtain widespread adoption motivates one alternative solution: a semi-centralized permissioned blockchain. We analyze that setting in Section 4.

Proposition 3.4. *Impossibility of Decentralization and Scalability*

[11] Our result highlights that, for example, theories attributing Bitcoin's limited adoption to its infancy fail to account for intrinsic economic limitations of the platform.

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

Our results may be interpreted as an economic parallel of Vitalik Buterin's Blockchain Trilemma.[12] 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 3.3 demonstrates that a secure PoW payments blockchain cannot scale in the sense that such a blockchain cannot realize high transaction volumes and non-negligible payments market share. Proposition 3.4 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 3.5. *No Latency, No Problem*
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 latency* $($*i.e.,* $\Delta(V) = 0)$*.*

Before transitioning to a discussion surrounding permissioned blockchains, we offer a final PoW result to demonstrate the importance of network latency in generating our results. Proposition 3.5 assumes, counterfactually, that network latency does not exist (i.e., $\Delta(V) = 0$) and thereby overcomes the Limited Adoption Problem. Widespread adoption becomes possible for a decentralized PoW system in the absence of latency which establishes that latency 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 con-

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

straint, free entry among validators and network latency that collectively make the system intrinsically impractical for widespread adoption. 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.

4 A Permissioned Alternative

Section 3 highlights that a PoW payments blockchain must centralize to overcome the Limited Adoption Problem. In this section, we consider a natural semi-centralized alternative: a permissioned blockchain. Section 4.1 formally puts forth the permissioned blockchain model. Section 4.2 establishes benefits of permissioned blockchains relative to PoW blockchains.

Nonetheless, those benefits are insufficient for blockchain to be viable. Typically, establishing blockchain security constitutes a necessary condition for blockchain viability. We consider that topic for permissioned blockchain in Sections 4.3 and 4.4. Section 4.3 introduces a standard consensus protocol and demonstrates that this protocol may incur successful attacks. Section 4.4 introduces an alternative protocol that overcomes both the Limited Adoption Problem and blockchain attacks.

4.1 Permissioned Blockchain Model

We model users as in Section 2 since the blockchain itself does not affect transaction demand. Unlike Section 2, we exogenously specify a set of validators, $V_P \in \mathbb{N}$.[13] 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.

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

PoW attempts to create incentives for validators not to maliciously attack the blockchain. Thus, in offering an alternative, we focus on not only user adoption and wait times 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.[14] We further define $\Gamma(a_1, ..., a_{V_P}, \alpha_1, ..., \alpha_{V_P}) \equiv \sum_{i=1}^{V_P} \omega_i(a_1, ..., a_{V_P}, \alpha_1, ..., \alpha_{V_P})\, a_i$. Γ gives the probability that the blockchain does not sustain a successful attack.

Saleh (2019) 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 sustains no 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 4.1. 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:

[14] The consensus protocol that we characterize arises as a simplification of the more general construct, specialized for our particular setting.

(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 4.1 defines a Permissioned Equilibrium.[15] Definition 4.1(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 4.1 (ii) requires that validators act optimally. We assume that all agents possess risk neutral preferences with perfect patience so that Definition 4.1 (iii) constitutes a necessary condition for equilibrium.

4.2 Permissioned Blockchain Benefits

Proposition 4.1. *Lower Payment Confirmation Times*
For any PoW protocol, there exists a permissioned blockchain which induces (weakly) lower payment confirmation times.

Section 3 demonstrates that PoW suffers from large payment confirmation times. This issue arises due to an artificial supply constraint and network latency 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 4.1 formalizes that assertion.

Proposition 4.2. *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.*

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

Section 3 establishes that PoW faces the Limited Adoption Problem. Proposition 4.2 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 4.2 avers, a permissioned blockchain may obtain widespread adoption.

4.3 Majority Rule Consensus

Definition 4.2. 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.[16] 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 4.3. *Majority Rule Permissioned Equilibrium* (*MRPE*)
For a Majority Rule Permissioned Equilibrium (*MRPE*), *the blockchain sustains a successful attack if and only if malicious validators weakly outnumber honest validators* (*i.e.* $\Gamma = \mathcal{I}\{|S_1| > |S_0|\}$).

Definition 4.2 specializes Definition 4.1 to a standard permissioned blockchain protocol. This standard permissioned blockchain protocol determines blockchain updates by a simple majority rule. Lemma 4.3 formalizes that assertion.

As established by Proposition 4.2, 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 4.4. *Honest MRPE*
There exists an MRPE in which all validators behave honestly and the blockchain does not sustain a successful attack (*i.e.*, $\forall i : a_i = 1, \Gamma = 1$).

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

Proposition 4.4 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 4.5. *Malicious MRPE*
There exists an MRPE in which all validators behave maliciously and the blockchain sustains a successful attack (*i.e,* $\forall i : a_i = 0, \Gamma = 0$).

Proposition 4.5 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 4.5 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 4.4 offers an alternative protocol that achieves both the desired goals.

4.4 Stake-Based Consensus

Definition 4.3. 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.[17] 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 $T_a \equiv \sum\limits_{i \in S_a} \alpha_i^+$.

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

Lemma 4.6. *Stake-Based Permissioned Equilibrium* (*SBPE*)

For a Stake-Based Permissioned Equilibrium (*SBPE*), *the blockchain sustains a successful attack if and only if the cumulative stake of malicious validators weakly outweighs that of honest validators* (*i.e.*, $\Gamma = \mathcal{I}\{T_1 > T_0\}$).

Definition 4.3 specializes Definition 4.1 to a permissioned blockchain protocol that we reference as a stake-based protocol. This protocol determines blockchain updates by majority stake rather than majority rule. Lemma 4.6 formalizes that result.

Proposition 4.7. *Honest SBPE*

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

Proposition 4.7 establishes the existence of an equilibrium in which all validators behave honestly. This equilibrium arises for similar reasons as that described within Proposition 4.4, so we omit further discussion.

Proposition 4.8. *No Malicious SBPE*

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

Proposition 4.8 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.

5 Conclusion

PoW blockchains have been envisioned as alternatives to traditional payment systems. While individual vendors have adopted some PoW payment platforms, no such platform has obtained widespread adoption. We demonstrate that this lack of widespread adoption constitutes an endemic property of PoW payments blockchains. PoW imposes an artificial supply constraint on transactions. As transaction demand grows, fees increase endogenously. Due to the permissionless nature of PoW blockchains, more validators engage in the validation process. That entry expands the network size thereby protracting the consensus process and generating increased payment confirmation times. Thus, only users extremely insensitive to wait-times transact via the blockchain in equilibrium. A PoW payments blockchain therefore cannot simultaneously sustain large volumes and a non-negligible market share - we term this result the Limited Adoption Problem.

We consider permissioned blockchains as an alternative to PoW blockchains. For any PoW blockchain, there exists a permissioned blockchain that dominates the PoW blockchain in terms of payment confirmation times. Permissioned blockchains, however, may generate malicious validator behavior. In fact, under a simple permissioned consensus protocol, an equilibrium with malicious validator behavior and a successful blockchain attack exists. We propose an alternative protocol that overcomes this undesirable feature. This protocol employs a cryptocurrency native to the blockchain to align validator incentives such that a blockchain attack cannot succeed in equilibrium.

This paper has important policy implications. It directly concerns adoption of blockchain as a payment system. The Limited Adoption Problem makes PoW 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.*

Basu, S., D. Easley, M. O'Hara, and E. Sirer (2019): "From Mining to Markets: The Evolution of Bitcoin Transaction Fees," *Working Paper.*

Biais, B., C. Bisière, M. Bouvard, and C. Casamatta (2019): "The Blockchain Folk Theorem," *Review of Financial Studies*, Forthcoming.

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.*

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.*

Cong, L. W., and Z. He (2019): "Blockchain Disruption and Smart Contracts," *Review of Financial Studies*, Forthcoming.

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

Cong, L. W., Y. Li, and N. Wang (2018): "Tokenomics: Dynamic Adoption and Valuation," *Working Paper*.

——— (2019): "Managing Tokenized Platforms," *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.

Dwork, C., and M. Naor (1992): "Pricing via processing or combatting junk mail," *In 12th Annual International Cryptology Conference*, pp. 139–147.

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*.

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*, Forthcoming.

Gandal, N., and H. Halaburda (2016): "Can we predict the winner in a market with network effects? Competition in the cryptocurrency market," *Games*, 7(3).

Gilad, Y., R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich (2017): "Algorand: Scaling Byzantine Agreements for Cryptocurrencies," *Proceedings of the 26th Symposium on Operating Systems Principles*, pp. 51–68.

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

Harvey, C. R. (2016): "Cryptofinance," *Working Paper.*

Hinzen, F. J. (2018): "Cryptocurrency Valuation: A Demand Side Approach," *Working Paper.*

Huberman, G., J. D. Leshno, and C. Moallemi (2018): "Monopoly without a Monopolist: 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, T., D. Shin, and B. Wang (2018): "Cryptocurrency Pump-and-Dump Schemes," *Working Paper.*

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

Makarov, I., and A. Schoar (2018): "Trading and Arbitrage in Cryptocurrency Markets," *Working Paper.*

Malinova, K., and A. Park (2018): "Tokenomics: When Tokens Beat Equity," *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.*

Nakamoto, S. (2008): "Bitcoin: A peer-to-peer electronic cash system," *https://bitcoin.org/bitcoin.pdf.*

Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder (2016): *Bitcoin and cryptocurrency technologies.* Princeton University Press.

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.

Niessner, M., S. T. Howell, and D. Yermack (2018): "Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales," *NBER Working Paper.*

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.*

Saleh, F. (2018): “Volatility and Welfare in a Crypto Economy,” *Working Paper.*

——— (2019): “Blockchain Without Waste: Proof-of-Stake,” *Working Paper.*

Sockin, M., and W. Xiong (2018): “A model of cryptocurrencies,” *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 $x \in X \equiv \{0, 1, ..., k\}$ with $x < k$ denoting that the blockchains last x heights contain single block and $x = k$ denoting the complement. Given the discussion in Section 2, $x < k$ corresponds to the blockchain being in the midst of a fork and $x = k$ 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, $\forall x \in X/\{0, k\} : Q_{x,x} = -\Lambda$, $\forall x \in X/\{0\} : Q_{x,0} = \Lambda p$, $\forall x \in X/\{k\} : Q_{x,x+1} = \Lambda(1 - p)$, $Q_{K,K} = -\Lambda p$, $Q_{0,0} = -\Lambda(1 - p)$ and all other entries equal 0.

Lemma A.1. *Stationary Distribution*

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

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

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

Proof.

We prove the result by induction. By definition, $\forall x \in X/\{k\} : s_x = 1 + (1-p)s_{x+1} + ps_0$ 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. $\forall x \in X/\{k\} : s_{x+1} \geqslant 0$ follows from $s_K = 0$. □

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

Proof.

We prove the result by induction. By definition, $\forall x \in X/\{k\} : s_x = 1 + (1-p)s_{x+1} + ps_0$ 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. $\forall x \in X/\{k\} : \frac{\partial s_{x+1}}{\partial\Lambda} \geqslant 0$ follows from $\frac{\partial s_K}{\partial\Lambda} = 0$. Symmetry of the functions, $\{s_X\}_{x\in X}$, implies $\forall x \in X/\{k\} : \frac{\partial s_x}{\partial\Delta(V)} > \frac{\partial s_{x+1}}{\partial\Delta(V)} \geqslant 0$ which completes the proof. □

We define $\tau \equiv \mathbb{E}[\sum\limits_{t=1}^{T_k} A_t]$ 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, $\tau = \tau(\Lambda, \Delta(V)) = \sum\limits_{x\in X}\frac{s_x(\Lambda,\Delta(V))}{\Lambda}\pi_x(\Lambda, \Delta(V))$.

Lemma A.5. *Lower Bound for τ*

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

Proof.

$\tau(\Lambda, \Delta(V)) \geqslant \Delta(V)\frac{s_0(\Lambda,\Delta(V))}{\Lambda\Delta(V)}\pi_0(\Lambda, \Delta(V)) = \Delta(V)\frac{e^{\Lambda\Delta(V)k}-1}{\Lambda\Delta(V)}$ 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*

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

Proof.

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

□

Lemma A.7. *Zero Wait*

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

Proof.

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

B Proofs

Proposition 2.1 *Existence and Uniqueness of a PoW Equilibrium*

There exists a PoW Equilibrium. There exists no other equilibrium for which f constitutes a strictly increasing and differentiable function. The following conditions characterize the equilibrium:

(A) $f(c_i) = (N-1)\frac{c_i^2}{2\Lambda}$

(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 $\tilde{V}(N, \Lambda, \beta) \equiv \frac{(N-1)N}{6\beta\Lambda}$ and $V^*(N, c^*, \Lambda, \beta) \equiv \frac{(N-1)N(c^*)^3}{6\beta\Lambda}$.

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 2.1 (iii) implies $\max\limits_{f_i \geqslant 0} R - c_i \cdot \mathbb{E}[W(f_i, f_{-i})|c_i] - f_i \geqslant R - c_i(\frac{N}{\Lambda} + \tau(\Lambda, V)) - f(c_i)$ so that Definition 2.1 (ii) yields $\forall c_i > 0 : R - c_i(\frac{N}{\Lambda} + \tau(\Lambda, V)) - f(c_i) \leqslant 0$. Then, right-continuity of f at 0 and Definition 2.1 (i) imply $R \leqslant 0$ which yields a contradiction and thereby eliminates such an equilibrium.

Problem 1 and Definition 2.1 (i) yield $\max_{f_i \geqslant 0} R - c_i \frac{(N-1)}{\Lambda} \mathbb{P}(f(c_j) \geqslant f_i \wedge c^* \geqslant c_j) - c_i \Psi(\Lambda, V) - f_i$. $f(c_i)$ being a strictly increasing function enables us to rewrite the latter problem as $\max_{f_i \geqslant 0} R - c_i \frac{(N-1)}{\Lambda} \max\{c^* - f^{-1}(f_i), 0\} - c_i \Psi(\Lambda, V) - f_i$. Differentiability of f then yields $\frac{c_i(N-1)}{\Lambda} \frac{1}{f'(f^{-1}(f_i))} = 1$ as a first-order condition for $c_i \in (0, c^*)$. In equilibrium, $f_i = f(c_i)$ so that the latter condition simplifies to $\frac{c_i(N-1)}{\Lambda} = f'(c_i)$ which in turn implies $f(c_i) = (N-1)\frac{c_i^2}{2\Lambda}$ over $f \in [0, c^*]$ when imposing $f(0) = 0$ and continuity of f. This result demonstrates that Proposition 2.1 (A) is necessary for the class of equilibria considered. Sufficiency for satisfying Definition 2.1 (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 2.1 (ii) and (iv) hold.

For $c^* \in (0, 1)$, Definition 2.1 (iv) equates with $V^*(N, c^*, \Lambda, \beta) = V$. Moreover, the continuous and strictly decreasing nature of $\max_{f_i \geqslant 0} R - c_i \cdot \mathbb{E}[W(f_i, f_{-i})|c_i] - f_i$ in c_i implies $R = c^* \Psi(\Lambda, V) + \frac{(c^*)^2(N-1)}{2\Lambda}$ via Definition 2.1 (ii). 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 2.1 (iv) so that $R \geqslant \Psi(\Lambda, \frac{(N-1)N}{6\beta\Lambda}) + \frac{N-1}{2\Lambda}$ by left-continuity of $\max_{f_i \geqslant 0} R - c_i \cdot \mathbb{E}[W(f_i, f_{-i})|c_i] - f_i$ and Definition 2.1 (ii). 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 2.1 and all other choices for V violate Definition 2.1 (iv).

□

Proposition 3.1 *Payment Confirmation Lower Bound*

Network latency 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 2.1 (D). Otherwise, Proposition 2.1 (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 2.1 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 3.2 *Arbitrarily Large Marginal 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 highest priority user, i.e., i such that* $c_i = c^*$*.*

Proof.

Proposition 3.1 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 3.3 *Limited 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 2.1 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 2.1 (B) yields $\lim_{N\to\infty} c^* = 0$ as desired. □

Proposition 3.4 *Impossibility of Decentralization and Scalability*

For exposition, we assume that $\lim_{N\to\infty}\Lambda$ and $\lim_{N\to\infty} c^*$ 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 $R, \beta > 0$, $2 \leqslant N_n \nearrow \infty$ and $\lim_{n\to\infty}\Lambda_n$ being well-defined in $\overline{\mathbb{R}}$. Then, following Proposition 2.1, 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 2.1 (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 2.1 (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 3.5 *No Latency, No Problem*

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 latency (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 latency). Note that this result does not contradict Proposition 3.4 as all parts of the paper (except this proposition) preclude $\Delta(V) = 0$ (i.e., we assume existence of network latency 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 2.1 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 4.1 *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 3.1. □

Proposition 4.2 *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 4.1 (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 4.3 *Majority Rule Permissioned Blockchain Equilibrium (MRPBE)*

For a Majority Rule Permissioned Blockchain Equilibrium (MRPBE), $\Gamma \equiv \mathcal{I}(|S(1)| > |S(0)|)$

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 4.4 *Honest MRPBE*

There exists an MRPBE in which all validators behave honestly and the blockchain does not sustain a successful attack

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 4.1 (i) and $P_0 = P_H$ satisfies Definition 4.1 (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 4.5 *Malicious MRPBE*

There exists an MRPBE in which all validators behave maliciously and the blockchain sustains a successful attack

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 4.1 (i) and $P_0 = P_L$ satisfies Definition 4.1 (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 4.6 *Stake-Based Permissioned Equilibrium (SBPE)*

For a Stake-Based Permissioned Equilibrium (SBPE), the blockchain sustains a successful attack if and only if the cumulative stake of malicious validators weakly outweighs that of honest validators (i.e., $\Gamma = \mathcal{I}\{T_1 > T_0\}$).

Proof.

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

Proposition 4.7 *Honest SBPE*

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

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 4.1 (i), and $P_0 = P_H$ satisfies Definition 4.1 (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, $\forall a \in \{0,1\}, \alpha \in \mathbb{R}$:

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

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

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

$$\leqslant 0$$

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

Proposition 4.8 *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 4.6, $\Gamma < 1 \implies \Gamma = 0$ which in turn implies $P_0 = P_L$ via Definition 4.1 (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. □