Blockchain Without Waste: Proof-of-Stake*

Fahad Saleh†
New York University, Stern

July 9, 2018

Abstract

A blockchain constitutes a distributed ledger that records transactions across a network of agents. Blockchain’s value proposition requires that agents eventually agree on the ledger’s contents since payments possess risk otherwise. Restricted blockchains ensure this consensus by appointing a central authority to dictate payment validity. Permissionless blockchains (e.g. Bitcoin, Ethereum), however, admit no central authority and therefore face a non-trivial issue of inducing consensus endogenously. Nakamoto (2008) provided a temporary solution to the problem by invoking an economic mechanism known as Proof-of-Work (PoW). PoW, however, lacks sustainability, so, in recent years, a variety of alternatives have been proposed. This paper studies the most famous such alternative, Proof-of-Stake (PoS). I provide the first formal economic model of PoS and demonstrate that PoS induces consensus in equilibrium. My result arises because I endogenize blockchain coin prices. Propagating disagreement introduces the prospect of default and thereby reduces blockchain coin value which implies that stake-holders face an implicit cost from delaying consensus. PoS randomly selects a stake-holder to update the blockchain and provides her an explicit monetary incentive, a “block reward,” for her service. In the event of disagreement, block rewards constitute a perverse incentive, but I demonstrate that restricting updating ability to large stake-holders induces an equilibrium in which consensus obtains as soon as possible. I also demonstrate that consensus obtains eventually almost surely in any equilibrium so long as the blockchain employs a modest block reward schedule. My work reveals the economic viability of permissionless blockchains.

Keywords: Blockchain, Consensus, Proof-of-Stake, FinTech, Cryptocurrency, Ethereum, Proof-of-Work, Bitcoin

JEL Classification: G00, G13

*I am especially grateful to Robert Engle, Joel Hasbrouck, Kose John, Thomas Philippon, Rangarajan Sundaram and David Yermack for extensive support and guidance. I also thank Farshid Abdi, Yakov Amihud, Matthieu Bouvard, William Cong, Manasa Gopal, Hanna Halaburda, Christopher Hennessy, Franz Hinzen, Burton Hollifield, Gur Huberman, Jiasun Li, Anthony Lynch, Andreas Park, Walter Pohl (discussant), Ioanid Rosu (discussant), Jacob Sagi, Alexi Savov, Robert Whitelaw and seminar participants at the Bergen FinTech 2018 Conference, Carnegie Mellon University, the Finance Theory Group Summer 2018 Conference, Indiana University, London Business School, McGill University, NYU Stern, the University of North Carolina, the WEAI 2018 Conference and the WFA 2018 Conference for valuable comments. All errors are my own.

†New York University - Leonard N. Stern School of Business, 44 West 4th St., NY 10012-1126 New York, USA. Email: fsaleh@stern.nyu.edu.
1 Introduction

A blockchain constitutes a distributed ledger that records transactions across a network of agents. Such a communal ledger possesses value only if agents agree on the ledger’s content. Consensus across agents may be achieved by appointing a central authority to dictate payment validity. Such a protocol describes a restricted blockchain. Philippon (2016) argues that “a restricted blockchain could in fact be used by incumbents to deter entry and stifle innovation” thereby “increase[ing] the rents of incumbents” but recognizes that “blockchain technology could improve... efficiency” otherwise. Thus, blockchain’s potential to improve financial market efficiency hinges upon the viability of permissionless (a.k.a. unrestricted) blockchains; this paper studies precisely that topic.

Figure 1: This figure compares annual energy consumption for Bitcoin and Ethereum with that for various countries. Retrieved from https://digiconomist.net/ethereum-energy-consumption.

A permissionless blockchain’s lack of a central authority renders the attainment of consensus a non-trivial issue. Nakamoto (2008) alleged to resolve that issue by employing an economic mechanism known as Proof-of-Work (PoW). PoW requires agents to compete to update the blockchain. The competition consists of solving a trivial puzzle so that success probabilities depend upon only raw computational power. An agent competes largely through
her energy expenditure, and PoW’s incentive structure led to an energy consumption explosion. Figure 1 ranks energy consumption by two PoW blockchains, Bitcoin and Ethereum, against that of all countries. The figure shows that Bitcoin and Ethereum collectively consume more energy on an annual basis than all but 69 countries individually. Separately, environmental researchers project that Bitcoin alone may overtake Denmark in energy consumption by 2020.¹

In hopes of creating a sustainable permissionless blockchain (i.e. one that does not expend an exorbitant amount of energy), the blockchain community has bandied about several alternatives to PoW. The most frequently discussed alternative is a mechanism known as Proof-of-Stake (PoS). PoS replaces PoW’s competition by offering a randomly selected stakeholder the authority to update the blockchain; PoS thus omits any incentive for agents to engage in a computational arms race. Developers, however, remain reluctant to employ PoS because they fear that PoS fails to induce consensus. PoS, like PoW, offers an agent an explicit monetary reward to update the blockchain, but PoS, unlike PoW, imposes no explicit cost upon agents to gain the authority to update the blockchain. Developers assert that an extant disagreement will persist indefinitely within a PoS blockchain because updating the blockchain, even if inconsistently, constitutes a weakly dominant strategy. This assertion is known as the Nothing-at-Stake problem, and it, if true, nullifies the viability of PoS.²

This paper’s first contribution is to provide the first formal economic model of PoS. Within that model, I subvert the Nothing-at-Stake problem thereby revealing PoS’s potential viability. My result requires endogenous pricing. A blockchain possess a native token or coin that facilitates exchange on that blockchain. A stake-holder of a given blockchain is an agent holding some coins of that blockchain. The Nothing-at-Stake problem implicitly assumes that an agent’s decision regarding whether to update the blockchain does not impact coin prices. I demonstrate the invalidity of this assumption. If an agent appends to the blockchain in a way that perpetuates disagreement then she imposes a cost upon all stake-holders because

¹ Bitcoin could consume as much electricity as Denmark by 2020
² I provide further detail regarding the Nothing-at-Stake problem within Section 2.3.
her action undercuts blockchain coins as a medium of exchange and thereby lowers the value of all such coins. PoS grants authority to update the blockchain to only stake-holders; thus, within PoS, an agent imposes a cost upon herself if she updates the blockchain in a manner that persists disagreement.

Invalidity of the Nothing-at-Stake problem need not imply that PoS obtains consensus. This paper, however, takes the next step and demonstrates general conditions under which PoS leads to consensus. That demonstration constitutes this paper’s second contribution. Formally, I show that restricting access to update the blockchain to sufficiently large stake-holders induces an equilibrium in which consensus obtains as soon as possible. This result arises because the cost of updating the blockchain in a manner that persists disagreement increases with an agent’s stake. For sufficiently large stake-holders, the cost of persisting disagreement outweighs the benefit from the explicit monetary reward given to agents updating the blockchain.

I also demonstrates that certain blockchain design choices imply that disagreement resolves eventually almost surely within any equilibrium. This result arises because indefinite disagreement nullifies the exchange value of blockchain coins and thus renders those coins worthless. If indefinite disagreement occurs with strictly positive probability then the conditional probability of indefinite disagreement must approach unity as time passes for paths with indefinite disagreement. On such paths, an agent eventually recognizes that her stake value will erode to zero, so she deviates thereby ensuring that such an equilibrium could not obtain.

**Related Literature**

Computer science contains a large literature that studies consensus. That literature dates back to Lamport, Shostak, and Pease (1982). More recent papers within that literature, with relevance to permissionless blockchains, include Miller and LaViola (2014), Chen and Micali (2016), Pass and Shi (2017) and Kiayias, Russell, David, and Oliynykov (2017). My paper differs from those works in that those papers rely upon exogenous behavioral assumptions.
whereas this paper employs the standard economic paradigm of implying agent behavior based on preferences, pay-offs and equilibrium analysis. Some computer science papers such as Eyal and Sirer (2014) and Nayak, Kumar, Miller, and Shi (2015) explicitly consider incentives but do not analyze equilibrium outcomes. Carlsten, Kalodner, Weinberg, and Narayanan (2016) conduct equilibrium analysis but only for PoW.

This paper also relates to a large practitioner literature that proposes PoS mechanisms that typically get implemented in live blockchains. That literature began with King and Nadal (2012) which put forth a hybrid PoS-PoW mechanism that Peercoin implemented. Nxt (2018) and Vasin (2013) followed with pure PoS mechanisms implemented by Nxt and Blackcoin respectively. More recently, Zhang (2018) puts forth a Byzantine Fault Tolerant (BFT) PoS mechanism implemented by NEO. This literature overlaps with the Computer Science consensus literature as Cardano implements Kiayias et al. (2017), a BFT PoS mechanism; Pass and Shi (2017) and Chen and Micali (2016) also constitute prominent PoS mechanisms. Prominent examples of PoS mechanisms proposed by practitioners that await implementation include Buterin and Griffith (2017) and Zamfir (2017). In contrast to the referenced papers, this paper studies a chain-based PoS mechanism akin to that discussed by Ethereum.\(^3\) This paper studies that simple implementation because this paper’s contribution centers around providing a formal economic equilibrium analysis, an analysis that the aforementioned papers fail to offer.


\(^3\)The interested reader may consult \url{https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs#what-is-proof-of-stake} for details.
The remainder of this paper is organized as follows. Section 2 introduces blockchain, PoW, PoS and the Nothing-at-Stake problem. Section 3 states the model. Section 4 invalidates the Nothing-at-Stake problem and proves that PoS achieves consensus under general conditions. Section 5 generalizes the model to enable free entry and demonstrates that the main results sustain. Section 6 demonstrates that the main results hold with an alternative definition of consensus. Section 7 concludes.

2 Background

2.1 Blockchain

A blockchain is a virtual chain of ordered blocks. Each block contains data and a reference to the previous block. Blocks may contain transactions (or be empty), and any transaction in a block must be valid given the preceding set of blocks. The blockchain receives an update only when a new block is appended to the end of the blockchain. New transactions enter the blockchain only by being included in a block that gets appended to the blockchain. Transactions on the blockchain are typically denominated in the currency of a native coin.

Figure 2: This figure depicts a blockchain with a single history.

Figure 2 depicts an example of a blockchain. The first block, Block 0, consists of only a single entry that records the wealth level of some agent, F. The following block, Block 1, then

---

4Actually, each block contains a reference to the previous block’s hash.

5For example, Bitcoin employs bitcoin coins (“bitcoins”) whereas Ethereum employs ether coins.
records an entry in which F spends F’s only dollar. This second entry points back to the first entry as a manner of validating that F has the wealth to pay SBUX. If F attempts to make a subsequent $1 payment to MCD then the blockchain will not accept that transaction because F cannot validate the transaction with a previous entry within the blockchain. Figure 2’s blockchain provides a unique history.

The blockchain community references a network state in which agents perceive different histories as a blockchain fork. Figure 3 depicts such a fork with the same transactions as Figure 2 but two histories. On the upper branch’s history, F paid SBUX $1; on the lower branch’s history, F paid MCD $1. Both histories acknowledge that F had only $1 initially, so neither branch will accept the transaction from Block 1 of the other branch. Both MCD and SBUX may worry about accepting F’s payment at face value and, if economically sensible, will haircut payments from a given branch on the basis of, among other things, the probability that the given branch eventually becomes accepted as the true history. This point highlights
the need for endogenous coin pricing, a topic that this paper discusses in Section 4.

2.2 Proof-of-Work (PoW)

Forks may arise for a variety of reasons, and a fork may appear without intent.\textsuperscript{6} Thus, ensuring that entries eventually become part of a blockchain’s unique accepted history necessitates having an effective consensus achievement process. To many within the blockchain community, PoW constitutes the only such viable process.


PoW extends beyond the scope of this paper, so I provide only a high-level discussion of the protocol.\textsuperscript{7} Appending a block to the blockchain entitles an agent to a block reward which consists of some blockchain coins. Some argue that if an agent may acquire an option to append to any blockchain branch without expense then forks will persist because acquiring and exercising the aforementioned option on all branches constitutes a weakly dominant strategy.\textsuperscript{8} PoW overcomes the presumed issue by requiring agents solve a puzzle to receive an option to append to a particular branch.\textsuperscript{9} Each branch possesses a different puzzle, and puzzles associated with branches from recent forks have similar difficulty. Biais et al. (2017) demonstrate that there exists an equilibrium in which agents co-ordinate and act on a single branch thereby resolving any extant fork via co-ordination. Solving one of the aforementioned puzzles, however, requires computational power, and PoW’s incentive structure triggered a computational arms race that manifests in an exorbitant level of energy expenditure by PoW

\textsuperscript{6}For example, many Bitcoin forks arise due to network latency.
\textsuperscript{7}The interested reader may consult Narayanan, Bonneau, Felten, Miller, and Goldfeder (2016) for a detailed discussion regarding PoW. Nakamoto (2008) also provides a description of the protocol.\textsuperscript{8}This description characterizes the Nothing-at-Stake problem. I provide additional detail later in this section.
\textsuperscript{9}Attempting to solve this puzzle is known as mining, and agents who mine are known as miners.
blockchains.

2.3 Proof-of-Stake (PoS)

PoS attempts to solve the energy expenditure problem created by PoW. To do so, PoS replaces PoW’s competition by randomly selecting stake-holders to append to the blockchain. The simplest implementation of PoS involves each blockchain branch selecting uniformly and randomly from the universe of blockchain coins. The owner of the selected coin then receives the option to append to the branch that selected her coin and simultaneously collect a reward. This protocol succeeds in reducing energy expenditure to negligible levels, but in doing so, PoS threatens to re-establish the problem ostensibly solved by PoW, the **Nothing-at-Stake** problem.

![Figure 4: Nothing-at-Stake problem. Retrieved from Ethereum Github.](image)

Figure 4 depicts the Nothing-at-Stake problem. One may view the act of appending to a branch of the blockchain as voting for that particular branch. Within that context, Figure 4 contends that PoS makes consensus impossible to achieve. This argument takes as given that each branch has some probability of becoming the unique history. The argument proceeds by asserting that appending blocks to all branches possible constitutes a weakly dominant strategy because all block rewards have non-negative value and agents obtain the right to append to the blockchain without expense.
Figure 4 considers the specific case of a two-branch fork. This setting assumes that Branch A and Branch B possess a 90% and 10% probability of resolving as the true history respectively. Figure 4 evaluates an agent’s pay-offs given that the agent receives the option to append a block to both branches. Although Branch A possesses a higher probability of resolving as the true history, the Nothing-at-Stake problem asserts that the agent will append blocks to both branches of the blockchain because this strategy yields a higher pay-off than appending a block to only Branch A. The stated argument exogenously imposes particular probabilities for a given branch to resolve as the true branch and then implicitly assumes that agent behavior does not affect coin prices. This paper takes the view that both coin prices and the aforementioned probabilities constitute endogenous quantities arising from the strategic choices of agents. Based on that view, this paper demonstrates that appending blocks to all branches imposes a cost upon an agent by reducing the value of blockchain coins. I formalize this point in Section 4.1.

3 Model

This paper primarily analyzes whether PoS achieves consensus. As a lack of consensus exists only if a blockchain fork persists, I model a fork and then evaluate if this fork persists under a PoS protocol. This section details the model.

3.1 Environment

I model an extensive form game with periods $t \in \mathbb{N}$. The game involves $N \geq 2$ players with $N \in \mathbb{N}$ and $I \equiv \{1, ..., N\}$. Player $i$ holds $\pi_i \in (0, 1)$ proportion of coins within the system at $t = 0$ with $\sum_{i=1}^{N} \pi_i = 1$. I let $S \in \mathbb{R}_{++}$ denote the total coin stock at $t = 0$. $\sum_{i=1}^{N} \pi_i = 1$ holds without loss of generality under the interpretation that this model analyzes a PoS protocol that restricts the set of agents with the ability to append to the blockchain.\[10

\[10\]In such a case, $\pi_i$ represents the proportion of coins held by Player $i$ among the $N$ players at $t = 0$, and $S$ represents the total number of coins held by those players at $t = 0$. 

9
3.2 PoS Protocol

I assume the blockchain employs a PoS protocol. This assumption implies that all periods $t \geq 1$ begin with each branch leaf node simultaneously and randomly selecting a coin from the set of coins owned by players. Any player who owns a drawn coin receives the option to append a block to the branch that drew her coin. All players receiving an option to extend a branch within any period act simultaneously during that period. Any player who receives that option in period $t$ earns $R_t \in \mathbb{R}_+$ in that period if she exercises her option. I assume that $\mathbb{R} \equiv \sup_{t \in \mathbb{N}} R_t < \infty$. No other activity occurs within a period, and the subsequent period commences immediately.

3.3 A Fork

I assume that a fork arises at $t = 0$. No further action occurs at $t = 0$, and the blocks that cause this fork involve no transactions. Then, this fork consists of two equally long branches at the end of $t = 0$.

3.4 Strategy Space

Each player’s strategy space consists entirely of whether or not that player opts to update the blockchain whenever called upon. More formally, Player $i$’s strategy space, $\mathcal{A}_i$, may be characterized by $\mathcal{A}_i \equiv \mathcal{A}_{1,i} \times \mathcal{A}_{2,i}$ with $\mathcal{A}_{b,i}$ denoting Player $i$’s actions when called upon to act by branch $b$. In turn, $\mathcal{A}_{b,i} \equiv \{ f : \mathcal{H}_{b,i} \mapsto \{0, 1\} \}$ with $\mathcal{H}_{b,i}$ denoting the instances in which branch $b$ calls upon Player $i$ to act, and $f(\cdot) = 0$ corresponds to Player $i$ not appending to the blockchain whereas $f(\cdot) = 1$ corresponds to Player $i$ appending to the blockchain. I provide a more formal treatment of the model’s strategy space within Appendix A.
3.5 Probability Space

The model’s only source of randomness arises from each branch randomly selecting a player at each time step. When the players play $\sigma \in \mathcal{A} \equiv \times_{i} \mathcal{A}_i$, I let $\pi_{i,b,t}^\sigma$ denote the proportion of coins within the system that Player $i$ holds on branch $b$ at the beginning of period $t$. Then, Player $i$’s probability of being selected by branch $b$ in time period $t$ equals $\pi_{i,b,t}^\sigma$. Moreover, branch 1’s draw is independent of branch 2’s draw. More formally, letting $X_{i,b,t}^\sigma$ denote the player selected on branch $b$ at time $t$, $\mathbb{P}\{X_{1,t}^\sigma = i_1, X_{2,t}^\sigma = i_2 | \mathcal{F}_{t-1}\} = \pi_{i_1,t}^\sigma \times \pi_{i_2,t}^\sigma$. I provide a more formal treatment of the model’s probability space within Appendix A.

3.6 Achieving Consensus

Narayanan et al. (2016) assert that forks resolve once “one of the two [branches] gets seen as more legitimate.” They assert that a branch gains legitimacy by becoming sufficiently longer than all other branches because the “chance that the shorter branch... will catch up to the longer branch becomes increasingly tiny as [the long branch] grows longer than any other branch.” Accordingly, I assume that the blockchain achieves consensus if and only if one branch exceeds the other branch by at least length $k \in \mathbb{N}$. I reference $k$ as the consensus threshold.

This “k-block rule” assumption possesses empirical support. Figure 5 depicts the frequency with which a branch eventually becomes part of the blockchain as the difference between the length of that branch and the length of the other branch.\textsuperscript{11} I show results only for $k = -6$ to $k = 6$ because the curve exhibits a monotonic relationship, equals 0 at $k = -6$ and equals 1 at $k = 6$. This graph highlights that, for the sample period, the main branch of the blockchain has not trailed any other branch by more than 6 blocks so that taking a lead of 6 blocks practically ensures that a branch will become the main branch.

I generate Figure 5 by scraping data from Blockchain.info. I employ the rvest package within R. Appendix C provides additional detail.

\textsuperscript{11}I restrict my attention to the two longest branches of the blockchain at any point in time.
Figure 5: This figure plots the frequency with which a branch eventually becomes part of the blockchain as the difference between the two longest branches varies. The data corresponds to the Bitcoin blockchain over blocks 350,000 - 450,000 (03/30/2015 - 01/25/2017). I provide detail regarding the data-gathering process in Appendix C.

I let $l_b^\sigma(t)$ denote the length of branch $b$ at the end of period $t$ when players play $\sigma$. I define $\Delta^\sigma(t) \equiv l_1^\sigma(t) - l_2^\sigma(t)$ so that $\Delta^\sigma(t)$ represents the gap between branches 1 and 2 at the end of period $t$. Then, $\tau^\sigma \equiv \inf\{t \in \mathbb{N} : |\Delta^\sigma(t)| \geq k\}$ represents the time at which the blockchain achieves consensus. If $\Delta^\sigma(\tau^\sigma) = k$ then I reference branch 1 as the winning branch since branch 1 possesses $k$ more blocks than branch 2 at time $\tau^\sigma$. Alternatively, if $\Delta^\sigma(\tau^\sigma) = -k$ then I reference branch 2 as the winning branch since branch 2 possesses $k$ more blocks than branch 1 at time $\tau^\sigma$.\footnote{If $\tau^\sigma = \infty$ then $\Delta^\sigma(\tau^\sigma)$ is not defined, so neither branch is the winning branch.} I invoke this “k-block rule” for the majority of this paper’s analysis, but I derive the main results of the paper without this “k-block rule” in Section 6.
3.7 Preferences, Pay-Offs and Equilibrium

I specify that all players possess risk-neutral preferences with a discount factor $\delta \in (0, 1)$. I assume that each coin earned on the winning branch confers upon the owner one consumption unit once the blockchain achieves consensus and that each coin generated on a losing branch confers no consumption value.

$$V_i^{(\sigma_i, \sigma_{-i})} = \sum_{b=1}^{2} \sum_{t=1}^{\infty} R_t Y_{b,t,i} A_{b,t,i}^{(\sigma_i, \sigma_{-i})} \delta^{(\sigma_i, \sigma_{-i})} t_{\leq t}^{(\sigma_i, \sigma_{-i})} = r_b^{(\sigma_i, \sigma_{-i})} + \delta^{(\sigma_i, \sigma_{-i})} \pi_i S$$  \hspace{1cm} (1)

$V_i^{(\sigma_i, \sigma_{-i})}$ constitutes the path-wise discounted pay-off for Player $i$ when she plays $\sigma_i$ and other players play $\sigma_{-i} \equiv \times_{j\in I: j \neq i} \sigma_j$. I assume that each player sells her stake and consumes upon consensus.\(^{13}\) $Y_{b,t,i}^{(\sigma_i, \sigma_{-i})}$ references the event that branch $b$ selects Player $i$ at time $t$. $A_{b,t,i}^{(\sigma_i, \sigma_{-i})}$ reflects Player $i$'s choice if called upon to act; $A_{b,t,i}^{(\sigma_i, \sigma_{-i})} = 1$ only if branch $b$ calls upon Player $i$ at time $t$, and Player $i$ opts to append. I abuse notation and let $r_b^{(\sigma_i, \sigma_{-i})}$ denote the period in which consensus obtains if branch $b$ wins when Player $i$ plays $\sigma_i$ and all other players play $\sigma_{-i}$.\(^{14}\)

$$\sigma^*_i \in \arg \sup_{\sigma_i \in \mathcal{A}_i} \mathbb{E}[V_i^{(\sigma_i, \sigma_{-i})}]$$  \hspace{1cm} (2)

Player $i$'s pay-off equals $\mathbb{E}[V_i^{(\sigma_i, \sigma_{-i})}]$ when Player $i$ plays $\sigma_i$ and all other players play $\sigma_{-i}$. Accordingly, $\{\sigma^*_i\}_{i=1}^{N}$ constitutes an equilibrium if $\sigma^*_i$ satisfies Equation 2 with $\sigma^*_j \equiv \times_{j \in I: j \neq i} \sigma^*_j$.

4 Main Results

This section provides the main results of this paper. Section 4.1 discusses pricing and highlights the fallacy within the Nothing-at-Stake problem. Section 4.2 establishes the existence of an equilibrium in which PoS obtains consensus and provides conditions under which all

\(^{13}\)All results hold if players sell coins prior to consensus. Moreover, selling upon consensus may be generated endogenously with a parameter restriction.

\(^{14}\)If branch $b$ does not win.
equilibria achieve consensus.

4.1 Not Nothing-at-Stake

For each branch $b$, time $t$ and set of strategies $\sigma$, I define $P^{\sigma}_{b,t} \equiv \mathbb{E}[^{\delta^{\tau_{\sigma} - t}}_{\tau_{\sigma} = \tau_{b}\tau} \mathcal{F}_t]$ if consensus occurs after time $t$. If consensus has already obtained, I take $P^{\sigma}_{b,t}$ as one if branch $b$ is the winning branch and zero otherwise.\(^\text{15}\) Then, $P^{\sigma}_{b,t}$ constitutes the ex-dividend price of a coin on branch $b$ at the end of time $t$ if players play $\sigma$. I reference $P^{\sigma}_{b,t}$ as ex-dividend because PoS potentially entitles the purchaser of a coin to additional coins in probability, and I term those additional coins as dividends of the purchased coin. For any economic agent not interested in appending to the blockchain (e.g. merchants), the ex-dividend price equates with the agent’s private valuation. Then, the ex-dividend price equals the price. Hereafter, I reference the ex-dividend price as the price without any qualification.

\[
\tilde{V}_i^{(\sigma_i,\sigma_{-i})} = \sum_{b=1}^{2} \sum_{t=1}^{\infty} \delta^{t} R_t Y^{(\sigma_i,\sigma_{-i})}_{b,t,i} A_{b,t,i}^{(\sigma_i,\sigma_{-i})} P_{b,t}^{(\sigma_i,\sigma_{-i})} \mathcal{I}_{\tau \in \tau^{(\sigma_i,\sigma_{-i})}} + \delta^{\tau_{\sigma_{-i}}} \pi_i S
\]  

Proposition 4.1. Pay-Off Equivalence

\[\forall i \in I, \sigma_i \in \mathcal{A}_i, \sigma_{-i} \in \mathcal{A}_{-i} : \mathbb{E}[V_i^{(\sigma_i,\sigma_{-i})}] = \mathbb{E}[\tilde{V}_i^{(\sigma_i,\sigma_{-i})}]\]

Corollary 4.2. Pay-Off Equivalence II

\[\forall i \in I, \sigma_i \in \mathcal{A}_i, \sigma_{-i} \in \mathcal{A}_{-i} : \mathbb{E}[V_i^{(\sigma_i,\sigma_{-i})}] = \sum_{b=1}^{2} \sum_{t=1}^{\infty} \delta^{t} R_t \mathbb{E}[Y^{(\sigma_i,\sigma_{-i})}_{b,t,i} A_{b,t,i}^{(\sigma_i,\sigma_{-i})} P_{b,t}^{(\sigma_i,\sigma_{-i})} \mathcal{I}_{\tau \in \tau^{(\sigma_i,\sigma_{-i})}}] + \pi_i S P_0^{(\sigma_i,\sigma_{-i})}\]

This paper’s main results do not depend upon the definition of $P^{\sigma}_{b,t}$. Nonetheless, the given definition yields an alternative interpretation of model pay-offs. Equation 3 provides path-wise discounted pay-offs for Player $i$ if Player $i$ sells coins as soon as she earns those coins and if she sells her entire stake upon consensus obtaining. $P_{b,t}^{(\sigma_i,\sigma_{-i})}$ constitutes an abuse of notation and references price when Player $i$ plays $\sigma_i$ and other players play $\sigma_{-i}$. Proposition 4.1 then highlights an equivalence between Section 3’s model and one that assumes the aforementioned

\(^{15}\text{More formally, } \forall b, t, \sigma : P^{\sigma}_{b,t} = \mathbb{E}[^{\delta^{\tau_{\sigma} - t}}_{\tau_{\sigma} = \tau_{\sigma}} \mathcal{F}_t] \mathcal{I}_{\tau_{\sigma} > t} + \mathcal{I}_{\tau_{\sigma} \leq t, \tau_{\sigma} = \tau_{\sigma}}\)
dynamics. This proposition does not imply that these two models provide identical results as the pay-off equivalence involves an abuse of notation with regard to the fact that, for example, $Y_{b,t,i}^{(\sigma_i,\sigma_{-i})}$ may possess a different probability law between the two model specifications. The results of Sections 4.2 and 6 apply to both models regardless.

Corollary 4.2 highlights the relationship between the Nothing-at-Stake problem and whether PoS achieves consensus. The Nothing-at-Stake problem concerns prices, but pay-offs depend upon prices. Thus, prior to turning to equilibrium analysis, I use the remainder of this subsection to subvert the Nothing-at-Stake problem. For exposition, I define $P_{\sigma}^t \equiv P_{1,t}^\sigma + P_{2,t}^\sigma$.

The Nothing-at-Stake problem alleges that players face no cost by deferring consensus. However, within a PoS protocol, all players with the ability to delay consensus own some coins, and delaying consensus reduces the value of those coins. The argument sketched within Section 2.3 treats coin value as exogenous and thereby arrives at a mistaken conclusion.

I define two particular strategies before formalizing the aforementioned argument. The first strategy, dubbed the **Longest Chain Rule** (hereafter referenced as the LCR), corresponds to a player appending only to the longest branch whenever feasible with the longest chain being defined as branch 1 whenever both branches possess the same length. The second strategy, dubbed the **Nothing-at-Stake strategy** (hereafter referenced as the NSS), corresponds to a player appending a block whenever given the option in line with the Nothing-at-Stake problem. Appendix A provides a formal definition for both these strategies. Hereafter, I let $LCR_{\sigma_i}^\sigma$ and $NSS_{\sigma_i}^\sigma$ reference strategies under which Player $i$ follows $\sigma_i$ until period $t$ and LCR and NSS respectively thereafter. Moreover, I define $LCR_{\sigma_i}^\sigma \equiv \times_{j \not= i} LCR_{\sigma_j}^\sigma$ and $NSS_{\sigma_i}^\sigma \equiv \times_{j \not= i} NSS_{\sigma_j}^\sigma$.

**Proposition 4.3. Not Nothing at Stake**

\[ \forall i \in I, (\sigma_i, \sigma_{-i}) \in \mathcal{A}_i \times \mathcal{A}_{-i}, \text{ at any time } t < \tau^{(\sigma_i, \sigma_{-i})} : \]
\[ P_t^{(\sigma_i, \sigma_{-i})} \leq P_t^{(LCR_{\sigma_i}^\sigma, LCR_{\sigma_{-i}}^\sigma)} \]
and
\[ 0 = P_t^{(NSS_{\sigma_i}^\sigma, NSS_{\sigma_{-i}}^\sigma)} < P_t^{(NSS_{\sigma_i}^\sigma, LCR_{\sigma_{-i}}^\sigma)} < P_t^{(LCR_{\sigma_i}^\sigma, LCR_{\sigma_{-i}}^\sigma)} \]
Proposition 4.3 avers that coin value obtains a maximum if all players follow LCR. This fact obtains because blockchain coins derive value from their ability to serve as a medium of exchange which in turn depends upon consensus obtaining expeditiously. As the blockchain achieves consensus at the earliest possible time when all players follow LCR, coin prices achieve a maximum in this case. Proposition 4.3 also states that following NSS instead of LCR when all other players follow LCR strictly reduces coin value. This finding undermines the Nothing-at-Stake problem as it establishes that following NSS imposes a cost upon stakeholders. Proposition 4.3 also asserts that all players following NSS causes coin price to achieve a minimum value of zero which further highlights that playing NSS imposes a cost upon players.

![March 2013 Fork](image)

Figure 6: This figure plots BTC prices through a fork on March 12th 2013. Prices come from [https://bitcoincharts.com/](https://bitcoincharts.com/).

Figure 6 provides empirical support. In March 2013, a fork arose on the Bitcoin blockchain, and the value of bitcoin collapsed as predicted by this section’s theory. Players reacted quickly
and migrated to one branch. This migration created consensus and restored value.

4.2 Equilibrium Analysis

This sub-section demonstrates that PoS achieves consensus under general conditions. I show existence of an equilibrium in which PoS achieves consensus as soon as possible. I also show that all equilibria obtain consensus eventually. Neither of these results hold without hypothesis which highlights that developers must heed economic guidance when designing PoS protocols for permissionless blockchains.

**Proposition 4.4. Immediate Consensus**

If \( \min_{i \in I} \pi_i \times S \geq \frac{R}{\delta^2 (1-\delta)^2} \), then there exists an equilibrium in which each player follows the longest chain rule. In such an equilibrium, the fork resolves at \( t = k \).

**Corollary 4.5. No Block Reward**

If \( \forall t \in \mathbb{N} : R_t = 0 \) then there exists an equilibrium in which each player follows the longest chain rule.

If a player appends to the blockchain, she receives a block reward. This block reward possesses non-negative value, but appending to the blockchain may defer consensus and thus decrease coin value. A myopic player with no coins always appends to the blockchain when given the option if the block reward takes a strictly positive value. Alternatively, a player with a large stake opts not to append to the blockchain when doing so defers consensus. Thus, an equilibrium in which all players follow the LCR exists if each player holds a sufficient stake. Proposition 4.4 formalizes that assertion.

Proposition 4.4 provides guidance to developers regarding designing a viable PoS blockchain. This proposition indicates that developers should restrict players with small stakes from appending to the blockchain. Having stake impels players to behave well. Moreover, the eligibility threshold for stake that ensures the existence of a symmetric LCR equilibrium depends upon the block reward level because a player must weigh her block reward against her pre-existing stake when deciding whether to append to the shorter branch.
Corollary 4.5 highlights a trivial but important insight: a permissionless blockchain need not possess a block reward. This result arises because a player incurs a cost for delaying consensus but receives no off-setting reward for appending to the blockchain’s shorter branch. If a player refuses to append to the blockchain’s longer branch when all other players play LCR then she delays consensus and thereby undermines her own wealth. If a player appends to the blockchain’s shorter branch when all other players play LCR then she also undermines her own wealth by delaying consensus, but she receives no block reward to counteract her loss. Thus, absent block rewards, an equilibrium in which all players follow LCR obtains without restricting the set of players with access to append to the blockchain. This finding demonstrates the practical significance of this paper’s insights.

**Proposition 4.6. No Never Consensus**

Let $\sigma^* \equiv \{\sigma^*_i\}_{i=1}^N \in \mathcal{A}$ denote an equilibrium. Then $\mathbb{P}\{\text{Consensus Never Obtains}\} \equiv \mathbb{P}\{\tau^{\sigma^*} = \infty\} < 1$.

Proposition 4.6 puts forth a simple but instructive result. If consensus never obtains with probability one then coin value equals zero almost surely. Moreover, since the model assumes bounded block rewards, player pay-offs must equal zero almost surely. Then, since playing LCR implies strictly positive pay-offs irrespective of the behavior of other players, no equilibrium possesses a zero probability of achieving consensus.

**Proposition 4.7. Eventual Consensus**

Let $\sigma^* \equiv \{\sigma^*_i\}_{i=1}^N \in \mathcal{A}$ denote an equilibrium. If $\sum_{t=1}^{\infty} R_t < \infty$ then $\mathbb{P}\{\text{Consensus Never Obtains}\} \equiv \mathbb{P}\{\tau^{\sigma^*} = \infty\} = 0$.

While trivial, Proposition 4.6 provides intuition that helps explain Proposition 4.7. Sample paths that never obtain consensus contribute nothing to player pay-offs. If Player $i$ perceives herself as being on such a path then she may deviate to LCR. Such a deviation ensures that consensus obtains with strictly positive probability in finite time which in turn implies a strictly positive pay-off contribution from the path. The difficulty within this argument
stems from the player accurately perceiving herself on a path that never obtains consensus. Nonetheless, if \( \lim_{t \to +\infty} P\{\text{Consensus Never Obtains} \} > 0 \) then \( \lim_{t \to +\infty} P\{\text{Consensus Obtains} | \text{No Consensus by } t \} = 0 \) so that as consensus fails to obtain at successive arbitrary horizons, a player eventually becomes more prone to perceiving herself as being on an undesirable path and therefore becomes more likely to deviate to LCR. This eventual deviation, however, implies the impossibility of an equilibrium in which consensus never obtains with strictly positive probability.

Proposition 4.7 re-iterates the advantage gained from PoS protocols providing modest block rewards. Block rewards provide perverse incentives for players to postpone consensus. Stake provides a countervailing incentive, but an overwhelming reward schedule may cause the perverse incentive to dominate. Thus, this result redoubles the need for developers to heed economic guidance when designing PoS protocols.

5 Endogenous Entry

In this section, I extend the results of Section 4 by allowing free entry. I augment the model of Section 3 by considering a set of arbitrarily many players, \( N \in \mathbb{N} \) and allowing each player to purchase coins immediately before period \( t = 0 \). Each player behaves as a price-taker, and the game unfolds as detailed in Section 3 thereafter. This section’s analysis, therefore, differs from the analysis of Section 4 because \( N \) and \( \{\pi_i\}_{i=1}^N \) constitute endogenous quantities.

\[
\mathbb{E}[V^{(\sigma_i, \sigma_{-i})}_i] - P \times S_i \quad (4)
\]

Prior to \( t = 0 \), players make entry decisions simultaneously by maximizing Equation 4 subject to \( S_i \geq 0 \) with \( S_i = \pi_i S \) denoting the Player \( i \)'s coin holding at \( t = 0 \) and \( P \) denoting the coin price immediately prior to \( t = 0 \). \( S_i \geq 0 \) denotes a short-selling constraint which aligns with the real-world implementation of major permissionless blockchains. \( V^{(\sigma_i, \sigma_{-i})}_i \) corresponds

\(^{16}\)I assume \( N < \infty \) for exposition. This assumption may be relaxed.
to the quantity defined in Equation 1 and implicitly depends upon \( S_i \). \( V_i^{(\sigma_i, \sigma_{-i})} \) also depends upon the PoS implementation being considered. For the remainder of this section, I follow Proposition 4.4 and consider a PoS implementation that restricts the set of players that may append to the blockchain to those holding at least \( S \equiv \frac{R}{\delta^2(1-\delta)^2} \) coins.

**Definition 5.1.** Given \( \delta, \{ R_i \}_{i=1}^n, \overline{N} \) and \( S \), a **Free Entry Equilibrium** denotes an initial price, \( P \), a set of initial stakes, \( \{ S_i^* \}_{i=1}^\overline{N} \), and a set of strategies contingent upon any set of initial stakes, \( \{ \tilde{\sigma}_i \}_{i=1}^\overline{N} \), such that:

(i) \( \forall i \text{ such that } S_i > 0 : \text{ Equation } 2 \text{ holds with } \sigma_i^* = \tilde{\sigma}_i(S_1^*, ..., S_{\overline{N}}^*) \)

(ii) \( \forall i : S_i^* \text{ maximizes Equation } 4 \text{ subject to } S_i \geq 0 \text{ with } \sigma_i = \tilde{\sigma}_i(S_1^*, ..., S_i, ..., S_{\overline{N}}^*) \)

and \( \sigma_{-i} = \prod_{j : j \neq i, S_j^* > 0} \tilde{\sigma}_j(S_1^*, ..., S_i, ..., S_{\overline{N}}^*) \)

(iii) \( \sum_{i=1}^{\overline{N}} S_i^* = S \)

Definition 5.1 defines a Free Entry Equilibrium. A Free Entry Equilibrium may be viewed as a sub-game perfect equilibrium in the sense that the analyzed setting constitutes an extensive form game with a sub-game for each set of simultaneous decisions, \( \{ S_i \}_{i=1}^\overline{N} \). Each sub-game corresponds to a game of the form described in Section 3 restricted to the set of entering players. In that context, \( \{ \tilde{\sigma}_i(S_1, ...S_{\overline{N}}) \}_{i : S_i > 0} \) being an Equilibrium in the sense defined within Section 3 for any \( \{ S_i \}_{i=1}^\overline{N} \), ensures that a Free Entry Equilibrium constitutes a sub-game perfect equilibrium as long as players make an optimal entry decision. Within Definition 5.1, (i) requires optimal behavior within each sub-game whereas (ii) requires an optimal entry decision; (iii) constitutes a market-clearing condition.

**Proposition 5.1.** LCR Free Entry Equilibria

\( P, \{ S_i^* \}_{i=1}^\overline{N} \) and \( \{ \tilde{\sigma}_i \}_{i=1}^\overline{N} \) constitute a Free Entry Equilibrium if the following conditions hold:

(i) \( \forall i : S_i^* \geq \overline{S} \lor S_i^* = 0 \)

(ii) \( P = \delta^k \left( \sum_{i=1}^{k} \frac{R_i}{S_i} + 1 \right) \)
(iii) \( \sum_{i=1}^{N} S_i^* = S \)

(iv) \( \forall i, \{S_i\}^N_{i=1} : \sigma_i(S_1, ..., S_N) \) corresponds to Player \( i \) playing LCR in the setting described within Section 3 with \( N = \sum_{i=1}^{N} I_{S_i > 0} \)

Proposition 5.1 characterizes a set of equilibria. Akin to Proposition 4.4, these equilibria feature each player playing the LCR. Different than Proposition 4.4, Proposition 5.1 examines free entry. Players enter by purchasing coins so that a player’s private coin valuation equaling coin value renders a player indifferent with respect to the entry decision. If all agents hold the same private coin valuation, the coin price equaling that valuation renders all agents indifferent across all feasible levels of coin holdings. A PoS implementation that enables only large stake-holders to append to the blockchain, however, causes private valuations for large stake-holders to differ from those of small stake-holders. This difference need not preclude the existence of an equilibrium because equilibrium prices may reflect the valuation of large stake-holders whereas other players face binding short sale constraints and hold no position in equilibrium. Within Proposition 5.1, (i) highlights that all players either hold large stakes or no stake; (ii) gives the large stake-holders’ coin valuation; (iii) imposes market-clearing, and (iv) ensures optimal behavior within each subgame.

**Corollary 5.2. Multiple Equilibria I**

Let \( N_{\text{max}} \equiv \frac{S^k(1-\delta)}{R} \). Then, if \( N_{\text{max}} > 2 \), there exist multiple equilibria in which only two players enter.

**Corollary 5.3. Multiple Equilibria II**

Let \( N_{\text{max}} \equiv \frac{S^k(1-\delta)}{R} \). Then, if \( N_{\text{max}} \geq 3 \), there exist equilibria with different numbers of entrants.

Corollaries 5.2 and 5.3 highlight that multiple equilibria result under mild conditions. Corollary 5.2 alludes to the existence of multiple equilibria in which two players enter. These equilibria differ in the initial coin holdings of each agent, but all such equilibria feature both agents purchasing at least \( \bar{S} \) coins. Corollary 5.3 requires stronger regularity than Corollary
5.2 but alludes to multiple equilibria that differ in the number of entrants. A player enters only if she can append to the blockchain and thereby accrue block rewards. However, since the market for coins must clear in equilibrium, equilibria with $N$ entrants arise only when at least $N\overline{S}$ coins exist; this requirement corresponds to the regularity demanded by Corollary 5.3.

6 Beyond $k$

This section considers an alternative definition for the consensus achievement moment. This definition does not rely on a “$k$-blocks rule.” Rather, I define fork resolution as the moment at which one branch receives no further blocks if the other branch continues to receive blocks. Appendix A provides a more formal description of this section’s model. With this section’s revised definition, I re-establish Propositions 4.3 and 4.4. I prove that Proposition 4.7 fails to obtain, but such a result may obtain if developers impose an analog of the “$k$-blocks rule” when specifying blockchain rules.

**Proposition 6.1. Not Nothing at Stake II**

$\forall i \in I, (\sigma_i, \sigma_{-i}) \in \mathcal{A}_i \times \mathcal{A}_{-i}$:

$p_t^{(\sigma_i, \sigma_{-i})} \leq p_t^{(LCR_{-i}^\sigma, LCR_{-i}^\sigma)}$

and

$0 = p_t^{(NSS_i^\sigma, NSS_{-i}^\sigma)} = p_t^{(NSS_i^\sigma, LCR_{-i}^\sigma)} < p_t^{(LCR_i^\sigma, LCR_{-i}^\sigma)}$

Proposition 6.1 affirms that the Not Nothing at Stake result holds under this sub-section’s set-up. As in Section 4.2, coin value obtains a maximum if all players follow LCR. Moreover, playing NSS instead of LCR when all other players play LCR strictly decreases coin value. Both these results arise because LCR ensures consensus achieves immediately whereas NSS delays consensus. These results re-affirm that the Nothing-at-Stake problem fails to obtain within a formal economic model.

**Proposition 6.2. Immediate Consensus II**
If $\min_{i \in I} \pi_i \times S \geq \frac{R_T}{\log \frac{1}{\delta}}$, then there exists an equilibrium in which each player follows the longest chain rule. In such an equilibrium, the fork resolves at $t = 0$.

**Corollary 6.3. No Block Reward**

If $\forall t \in \mathbb{N} : R_t = 0$ then there exists an equilibrium in which each player follows the longest chain rule.

Proposition 6.2 establishes the existence of an equilibrium in which all players play LCR. As in Section 4.2, appending to the shorter branch delays consensus and thereby reduces coin value. This coin value reduction is especially costly for players with large stakes. Accordingly, if a PoS protocol permits only sufficiently large stake-holders to append to the blockchain then a symmetric LCR equilibrium arises. As in Section 4.2, if the blockchain possesses no block rewards then the symmetric LCR equilibrium obtains without restricting the set of players with access to append to the blockchain.

**Proposition 6.4. Never Consensus**

There exists an equilibrium in which each player follows the Nothing-at-Stake strategy. In such an equilibrium, the fork never resolves with probability one.

Proposition 6.4 reveals that Propositions 4.6 and 4.7 fail under this sub-section’s set up. This failure reflects the inability of agents to unilaterally impose consensus with strictly positive probability. If a particular player plays NSS then all players receive a pay-off of zero irrespective of the action of any other player. Thus, each player playing NSS constitutes an equilibrium.

<table>
<thead>
<tr>
<th>Player 1</th>
<th>Player 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSS</td>
<td>$\sigma_2$</td>
</tr>
<tr>
<td></td>
<td>${E[V_1^{(\sigma_1,\sigma_2)}], E[V_2^{(\sigma_2,\sigma_1)}]}$</td>
</tr>
<tr>
<td></td>
<td>$(0,0)$</td>
</tr>
</tbody>
</table>

Table 1: Heuristic Normal Form with $N = 2$
Table 1 provides a heuristic normal form representation of the game with $N = 2$. Although the bottom right box provides the lowest possible pay-offs, this cell nonetheless constitutes an equilibrium. This result arises because all unilateral deviations from the bottom right also produce the lowest possible pay-off.

Proposition 6.4 indicates that a PoS-blockchain requires additional economic structure to ensure that arbitrary equilibria obtain consensus eventually almost surely. Proposition 4.7 suggests that allowing players to unilaterally deviate to induce consensus with strictly positive probability facilitates such a property. Thus, obtaining a result such as Proposition 4.7 may require developers to build a “k-blocks rule” into the blockchain protocol.

7 Conclusion

This paper provides the first formal economic analysis of PoS. I demonstrate that PoS achieves consensus under general conditions. Therefore, my work highlights that developers may implement a viable permissionless blockchain without prohibitive energy consumption.

My results do not validate arbitrary PoS implementations. Rather, my conclusions emphasize the need for developers to heed economic guidance when designing consensus protocols. For PoS, stake constitutes an important attribute. An agent with negligible stake may delay consensus by seeking block rewards. In contrast, an agent with a large stake undermines her own wealth when postponing consensus even if such behavior yields block rewards. Blockchain developers, therefore, should restrict the set of agents with an ability to append to the blockchain in line with the blockchain’s reward schedule. As the block reward schedule becomes more modest, the necessary restriction becomes more lax.

Even setting aside exorbitant energy expenditure levels, Budish (2018) raises concerns regarding the economic viability of PoW blockchains. Such concerns highlight the need for research regarding the economic viability of non-PoW mechanisms. This paper begins to fill that need.
References


Miller, A., and J. J. LaViola. 2014. Anonymous Byzantine Consensus from Moderately-


Appendices

A  Model

A.1  Strategy Space

I characterize period $t$’s observable events by $h \in h_t$ with $\forall t \in \mathbb{N} : h_t \equiv I^2 \times \{0,1\}^2$. The first two elements reference the owner of the coin drawn in period $t$ whereas the last two elements reference whether or not each branch received a new block in the same period. More formally, $\forall t \in \mathbb{N} : h_t = (i_1, i_2, x_1, x_2)$ represents the following proposition: $\forall b \in \{1,2\}, i \in I$: branch $b$ drew Player $i$’s coin in period $t$ $\land$ Player $i$ exercised her option $\iff i_b = i \land x_b = 1$. $H_t \in \mathcal{H}_t \equiv \times_{s=1}^{t-1} h_s \times I^2$ characterizes the observable history prior to any period-$t$ player action. This specification implies that, when deciding whether to append to the blockchain in period $t$, a player knows not only the entire structure of the blockchain but also which players received the option to append to each branch in previous periods and which players hold options to append to the blockchain in the current period. Additionally, I characterize Player $i$’s action space as $A_i \equiv A_{1,i} \times A_{2,i}$ with $A_{b,i} \equiv \{ f : \mathcal{H}_{b,i} \rightarrow \{0,1\} \}$ and $\mathcal{H}_{b,i} \equiv \bigcup_{t=0}^{\infty} \{ H \in \mathcal{H}_{t+1} : H_{4t+b} = i \land \max\{ \bigcup_{s \in \mathbb{N}, 1 \leq s \leq t} |\sum_{j=0}^{s-1} (H_{4j+3} - H_{4j+4})| \} \bigcup \{0\} < k \}$. Player $i$ taking action $(f_1, f_2) \in A_i$ asserts the proposition $\forall b \in \{1,2\} : \forall H \in \mathcal{H}_{b,i} :$ Player $i$ appends to branch $b$ given history $H$ if and only if $f_b(H) = 1$.

A.2  Probability Model

I model the game on a triple, $(\Omega, \mathcal{F}, \mathbb{P})$, generated by two independent sequences of i.i.d random variables, $\{U_{1,t}\}_{t=1}^{\infty}$ and $\{U_{2,t}\}_{t=1}^{\infty}$, with each variable being distributed $U[0,1]$. $U_{b,t}$ represents a draw of a coin for branch $b$ in period $t$. By construction, $\forall \sigma \in \mathcal{A} \equiv \times_{i=1}^{N} \mathcal{A}_i, t_0 < t_1, (i_1, i_2) \in I^2 : \mathbb{P}\{ \bigcap_{b=1}^{2} \{ X_{b,t_1} = i_b \} \mid \mathcal{F}_{t_0} \} = \mathbb{E}[\pi_{i_1, t_1} \pi_{i_2, t_1} \mid \mathcal{F}_{t_0}]$ with $\pi_{i_{1,2},t}$ denoting the proportion of coins within the system that Player $i$ possesses on branch $b$ at the beginning of time $t$ and
$X_{b,t}^\sigma$, denoting the owner of the coin drawn on on branch $b$ in period $t$. Both $\pi_{i,b,t}^\sigma$ and $X_{b,t}^\sigma$ depend on the strategy set $\sigma \in \mathcal{A}$.

A.3 Strategies

\forall i \in I, I define $\Delta_i : \mathcal{H}_{1,i} \cup \mathcal{H}_{2,i} \to \mathbb{N}$ such that $\forall i \in I : H \in \mathcal{H}_{1,i} \cup \mathcal{H}_{2,i} : \Delta_i(H) \equiv \sum_{t=0}^{\lfloor \mu \rfloor - 6} (H_{4i+3} - H_{4i+4})$. For Player $i$, the LCR corresponds to $LCR_i \equiv (f_{1,i}, f_{2,i}) \in \mathcal{A}_i$ such that $\forall H_1 \in \mathcal{H}_{1,i}, H_2 \in \mathcal{H}_{2,i} : f_{1,i}(H_1) = \mathcal{I}_{\Delta_i(H_1) \geq 0} \land f_{2,i}(H_2) = \mathcal{I}_{\Delta_i(H_2) < 0}$. For Player $i$, the NSS corresponds to $NSS_i \equiv (g_{1,i}, g_{2,i}) \in \mathcal{A}_i$ such that $\forall H_1 \in \mathcal{H}_{1,i}, H_2 \in \mathcal{H}_{2,i} : g_{1,i}(H_1) = 1 \land g_{2,i}(H_2) = 1$.

A.4 Beyond $k$

Section 6 maintains the structure of Section 3 except that I redefine $\mathcal{H}_{b,i}$, $\tau_b^\sigma$ and $\tau^\sigma$. I define $\mathcal{H}_{b,i} \equiv \bigcup_{t=0}^{\infty} \{ H \in \mathcal{H}_{i+1} : H_{4t+b} = i \}$. Moreover, I define $\tau_b^\sigma \equiv \inf\{ t \in \mathbb{N} \cup \{0\} : l_{3-b}^\sigma(t) = \lim_{n \to \infty} l_{3-b}^\sigma(n) \}$ if $\lim_{n \to \infty} l_{3-b}^\sigma(n) = \infty$ and $\tau_b^\sigma \equiv \infty$ otherwise. I also define $\tau^\sigma \equiv \min\{ \tau_1^\sigma, \tau_2^\sigma \}$. These revised definitions imply that merchants accept a coin at face value if and only if the coin’s branch processes transactions forevermore and the other branch processes no further transactions. Players and pay-offs remain as given in Section 3.

B Proofs

Proposition 4.1 Pay-Off Equivalence

$\forall i \in I, \sigma_i \in \mathcal{A}_i, \sigma_{-i} \in \mathcal{A}_{-i} : \mathbb{E}[\tilde{V}_t^{(\sigma_i, \sigma_{-i})}] = \mathbb{E}[V_t^{(\sigma_i, \sigma_{-i})}]$

Proof.

$\forall b \in \{1, 2\}, t \in \mathbb{N}, i \in I, \sigma_i \in \mathcal{A}_i, \sigma_{-i} \in \mathcal{A}_{-i} :$

$\mathbb{E}[\delta^t R_t Y_{b,t,i}^{(\sigma_i, \sigma_{-i})} A_{b,t,i}^{(\sigma_i, \sigma_{-i})} P_{b,t}^{(\sigma_i, \sigma_{-i})} \mathcal{I}_{t \leq \tau(\sigma_i, \sigma_{-i})}]$

$= \mathbb{E}[\delta^t R_t Y_{b,t,i}^{(\sigma_i, \sigma_{-i})} A_{b,t,i}^{(\sigma_i, \sigma_{-i})} \mathbb{E}[\delta^{\tau(\sigma_i, \sigma_{-i})-\tau(\sigma_i, \sigma_{-i})} \mathcal{I}_{\tau(\sigma_i, \sigma_{-i}) = \tau_b^{(\sigma_i, \sigma_{-i})}} | \mathcal{F}_t] \mathcal{I}_{t \leq \tau(\sigma_i, \sigma_{-i})}]$

$= \mathbb{E}[R_t Y_{b,t,i}^{(\sigma_i, \sigma_{-i})} A_{b,t,i}^{(\sigma_i, \sigma_{-i})} \delta^{\tau(\sigma_i, \sigma_{-i})} \mathcal{I}_{t \leq \tau(\sigma_i, \sigma_{-i}) = \tau_b^{(\sigma_i, \sigma_{-i})}}]$
The last equality follows from the law of iterated expectation and measurability of
$R_t Y^{(σ_i,σ_{−i})} A^{(σ_i,σ_{−i})}_b,t,i I_{t<τ^{(σ_i,σ_{−i})}=σ_i}$ with respect to $F_t$. Then, Monotone Convergence Theorem and linearity of expectation yield the desired result. □

**Proposition 4.3 Not Nothing at Stake**

∀i ∈ I, (σ_i, σ_{−i}) ∈ $A_i ×$ $A_{−i}$, at any time $t < τ^{(σ_i,σ_{−i})}$:

$P_t^{(σ_i,σ_{−i})} ≤ P_t^{(LCR_i,t,LCR_{−i})}$

and

$0 = P_t^{(NSS_i,t,NSS_{−i})} < P_t^{(NSS_i,t,LCR_{−i})} < P_t^{(LCR_i,t,LCR_{−i})}$

**Proof.**

∀ω ∈ Ω, i ∈ I, (σ_i, σ_{−i}) ∈ $A_i ×$ $A_{−i}$:

$t < τ^{(σ_i,σ_{−i})}$ implies $τ^{(σ_i,σ_{−i})} ≥ \min \{k − Δ^{(σ_i,σ_{−i})}(t), Δ^{(σ_i,σ_{−i})}(t) + k\} + t = τ^{(LCR_i,t,LCR_{−i})}$ which implies $P_t^{(σ_i,σ_{−i})} ≤ P_t^{(LCR_i,t,LCR_{−i})}$.

Further, $t < τ^{(σ_i,σ_{−i})}$ implies $τ^{(NSS_i,t,NSS_{−i})} = \infty$, $P\{τ^{(NSS_i,t,LCR_{−i})} > t + k|F_t\} > 0$ and $P\{τ^{(NSS_i,t,LCR_{−i})} < \infty|F_t\} > 0$ so that $R < \infty$ yields $0 = P_t^{(NSS_i,t,NSS_{−i})} < P_t^{(NSS_i,t,LCR_{−i})} < P_t^{(LCR_i,t,LCR_{−i})}$ as desired. □

**Proposition 4.4 Immediate Consensus**

If $\min_{i∈I} π_i × S ≥ \frac{R}{k(1−δ)^2}$, then there exists an equilibrium in which each player follows the longest chain rule. In such an equilibrium, the fork resolves at $t = k$.

**Proof.**

∀i ∈ I, σ_i ∈ $A_i$: I let $d_t^ω$ denote a random variable that equals the first period that $σ_i$ differs from $LCR_i$ on the path of play when all other players play $LCR_i$. ∀i ∈ I : ∀σ_i ∈ $A_i$ :

$V_i^{(LCR_i,t,LCR_{−i})} I_{d_t^ω > k} = V_i^{(σ_i,t,LCR_{−i})} I_{d_t^ω > k}$ so that $E[V_i^{(LCR_i,t,LCR_{−i})} I_{d_t^ω ≤ k}] ≥ E[V_i^{(σ_i,t,LCR_{−i})} I_{d_t^ω ≤ k}]$ suffices to prove the desired conclusion.

∀i ∈ I, σ_i ∈ $A_i$: I define $Λ_i^{σ_i} = \{ω ∈ Ω : \{Y_{1,i}^{(σ_i,t,LCR_{−i})} Y_{2,i}^{(σ_i,t,LCR_{−i})} A_{1,i}^{(σ_i,t,LCR_{−i})} (1 − A_{1,i}^{(σ_i,t,LCR_{−i})}) = 1\}] \cap \{Y_{1,i}^{(σ_i,t,LCR_{−i})} A_{1,i}^{(σ_i,t,LCR_{−i})} = 0\} \cap \{Y_{2,i}^{(σ_i,t,LCR_{−i})} (1 − A_{2,i}^{(σ_i,t,LCR_{−i})}) = 0\}$ and $Λ_i = \{ω ∈ Ω : Y_{1,i}^{(LCR_i,t,LCR_{−i})} Y_{2,i}^{(LCR_i,t,LCR_{−i})} = 1\}$. 

30
Then,
\[
\mathbb{E}[V^i(\sigma_i, LCR_{-1}) \mathcal{L}_{d_i^t \leq k}]
\leq \mathbb{E}[V^i(\sigma_i, LCR_{-1}) \mathcal{L}_{d_i^t \leq k \cap \Lambda_i^t}] + (\frac{R}{1-\delta} + \delta^{k+1} \pi_i S) \mathbb{P}\{d_i^t \leq k\} \cap (\Lambda_i^t)\]
\leq \delta^k \mathbb{E}\left[\sum_{t=1}^{k} R_t Y_{2,t,i} \sigma_i, LCR_{-1} A_{2,t,i} \mathcal{L}_{d_i^t \leq k \cap \Lambda_i^t}\right] + \delta^k \pi_i S \mathbb{P}\{d_i^t \leq k\}.
\]
The second inequality follows from \(\min_{i \in I} \pi_i \times S \geq \frac{R}{\delta(1-\delta)^2}\).

Additionally,
\[
\mathbb{E}[V^i(LCR_i, LCR_{-1}) \mathcal{L}_{d_i^t \leq k}]
\geq \mathbb{E}[V^i(LCR_i, LCR_{-1}) \mathcal{L}_{d_i^t \leq k \cap \Lambda_i} \cap \Lambda_i]
+ \delta^k \pi_i S \mathbb{P}\{d_i^t \leq k\} \cap \Lambda_i
\geq \delta^k \mathbb{E}\left[\sum_{t=1}^{k} R_t Y_{1,t,i} \sigma_i, LCR_{-1} A_{1,t,i} \mathcal{L}_{d_i^t \leq k \cap \Lambda_i}\right] + \delta^k \pi_i S \mathbb{P}\{d_i^t \leq k\}.
\]

If \(\Lambda_i^t = \emptyset\) then the result follows immediately. Otherwise, let \(\sigma_i^t \in \mathcal{A}_i\) denote a strategy such that Player \(i\) follows \(\sigma_i\) at \(t = 1\) and then LCR thereafter. Then,
\[
\mathbb{E}\left[\sum_{t=1}^{k} R_t Y_{2,t,i} \sigma_i, LCR_{-1} A_{2,t,i} \mathcal{L}_{d_i^t \leq k \cap \Lambda_i^t}\right] = \mathbb{E}\left[\sum_{t=1}^{k} R_t Y_{2,t,i} \sigma_i, LCR_{-1} A_{2,t,i} \mathcal{L}_{d_i^t \leq k} \cap \Lambda_i^t\right]
\leq \mathbb{E}\left[\sum_{t=1}^{k} R_t Y_{1,t,i} \sigma_i, LCR_{-1} A_{1,t,i} \mathcal{L}_{d_i^t \leq k} \cap \Lambda_i^t\right] = \mathbb{E}\left[\sum_{t=1}^{k} R_t Y_{1,t,i} \sigma_i, LCR_{-1} A_{1,t,i} \mathcal{L}_{d_i^t \leq k} \cap \Lambda_i^t\right]
\]
which completes the proof.
Proposition 4.6 No Never Consensus

Let $\sigma^* \equiv \{\sigma_i^*\}_{i=1}^N \in A$ denote an equilibrium. Then $\mathbb{P}\{\text{Consensus Never Obtains}\} \equiv \mathbb{P}\{\tau^{\sigma^*} = \infty\} < 1$.

Proof.

By contradiction, suppose there exists an equilibrium strategy set, $\sigma^* \equiv \{\sigma_i^*\}_{i=1}^N \in A$, such that $\mathbb{P}\{\tau^{\sigma^*} = \infty\} = 1$. Then, $\forall i \in I : \mathbb{E}[V_i^{(\sigma^*_i, \sigma^*_{\neq i})}] = \mathbb{E}[V_i^{(\sigma^*_i, \sigma^*_{\neq i})}]_{\tau^{\sigma^*} = \infty}$. Moreover, $\forall i \in I : V_i^{(\sigma^*_i, \sigma^*_{\neq i})}_{\tau^{\sigma^*} = \infty} \leq \lim_{t \to \infty} \{2t\delta R + \delta t \pi_i S\} = 0$ so that $\forall i \in I : V_i^{(\sigma^*_i, \sigma^*_{\neq i})}_{\tau^{\sigma^*} = \infty} = 0$ which implies $\forall i \in I : \mathbb{E}[V_i^{(\sigma^*_i, \sigma^*_{\neq i})}] = 0$. Then, $\forall i \in I : \mathbb{E}[V_i^{(LCR, \sigma^*_{\neq i})}] > 0$ delivers the desired contradiction thereby completing the proof.

Proposition 4.7 Eventual Consensus

Let $\sigma^* \equiv \{\sigma_i^*\}_{i=1}^N \in A$ denote an equilibrium. If $\sum_{t=1}^{\infty} R_t < \infty$ then $\mathbb{P}\{\text{Consensus Never Obtains}\} \equiv \mathbb{P}\{\tau^{\sigma^*} = \infty\} = 0$.

Proof.

$\forall i \in I, t \in \mathbb{N}$, I define strategy $\sigma_{i,t} \in A_i$ such that Player $i$ follows $\sigma_i^*$ until period $t$ and LCR thereafter. Then, $\forall i \in I, t \in \mathbb{N} : \mathbb{E}[V_i^{(\sigma_i^*, \sigma_{\neq i})}] \geq \mathbb{E}[V_i^{(\sigma_i^*, \sigma_{\neq i})}]_{\tau^{\sigma^*} \leq t} = V_i^{(\sigma_i^*, \sigma_{\neq i})}_{\tau^{\sigma^*} \leq t}$ so that $\mathbb{E}[V_i^{(\sigma_i^*, \sigma_{\neq i})} $_{$\tau^{\sigma^*} > t}$] $\geq \mathbb{E}[V_i^{(\sigma_i^*, \sigma_{\neq i})}$_{$\tau^{\sigma^*} > t}$]$. Direct verification reveals that $\mathbb{E}[V_i^{(\sigma_i^*, \sigma_{\neq i})}$_{$\tau^{\sigma^*} > t}$] $\leq \delta t \times \mathbb{P}\{t < \tau^{\sigma^*} < \infty\} \times (\sum_{s=1}^{t} R_s + \frac{R_0}{1-\delta} + \pi_i S)$ and $\mathbb{E}[V_i^{(\sigma_i^*, \sigma_{\neq i})}$_{$\tau^{\sigma^*} > t}$] $\geq \delta^{t+k} \times \mathbb{P}\{\tau^{\sigma^*} > t\} \pi_i^{2k} \times \pi_i S$ with $\pi_i \equiv \frac{\pi_i S}{S + \sum_{t=1}^{\infty} R_t}$. Thus, $\forall i \in I, t \in \mathbb{N}$:

$\mathbb{P}\{\tau^{\sigma^*} > t\} \leq \frac{\mathbb{P}\{t < \tau^{\sigma^*} < \infty\} \times \left( \sum_{s=1}^{t} R_s + \frac{R_0}{1-\delta} + \pi_i S \right) \delta^{t+k} \times \pi_i S}{\delta^{t+k} \times \pi_i S}$ so that taking limits as $t \to \infty$ on both sides yields $\mathbb{P}\{\tau^{\sigma^*} = \infty\} = 0$ as desired.

Proposition 5.1 LCR Free Entry Equilibria

$P, \{S_i^*\}_{i=1}^N$ and $\{\bar{S}_i\}_{i=1}^N$ constitute a Free Entry Equilibrium if the following conditions hold:

(i) $\forall i : S_i^* \geq \bar{S} \lor S_i^* = 0$
(ii) \( P = \delta^k \left( \sum_{t=1}^{k} \frac{R_t}{S} + 1 \right) \)

(iii) \( \sum_{i=1}^{N} S^*_i = S \)

(iv) \( \forall i, \{S_i\}_{i=1}^{N} : \sigma_i(S_1, ..., S_N) \) corresponds to Player \( i \) playing LCR in the setting described within Section 3 with \( N = \sum_{i=1}^{N} I_{S_i > 0} \)

**Proof.**

Proposition 5.1 (iv) and (iii) ensure Definition 5.1 (ii) and (iii) by Proposition 4.4. Thus, I need only demonstrate that Proposition 5.1 (i) and (ii) ensure Definition 5.1 (ii).

I assume that Players take the total set of active coins, \( S \), as given. Then, Equation 4 becomes a piece-wise linear optimization problem in \( S_i \) with slope \( \delta^k - P \) for \( S_i < \overline{S} \) and slope \( \delta^k \left( \sum_{t=1}^{k} \frac{R_t}{S} + 1 \right) - P \) for \( S_i \geq \overline{S} \). Then, 5.1 (ii) ensures that Equation 4 possesses a maximum of 0 which obtains if \( S_i = 0 \) or \( S_i \geq \overline{S} \) so that 5.1 (i) and (ii) imply Definition 5.1 (ii) as desired.
**Proposition 6.1 Not Nothing at Stake II**

\[ \forall i \in I, (\sigma_i, \sigma_{-i}) \in A_i \times A_{-i}: \]

\[ P_t^{(\sigma_i, \sigma_{-i})} \leq P_t^{(LCR_i, LCR_{-i})} \]

and

\[ 0 = P_t^{(NSS_i, NSS_{-i})} = P_t^{(NSS_i, LCR_{-i})} < P_t^{(LCR_i, LCR_{-i})} \]

**Proof.**

\[ \forall \omega \in \Omega, i \in I, (\sigma_i, \sigma_{-i}) \in A_i \times A_{-i}: \]

\[ \tau^{(LCR_i, LCR_{-i})} \leq t \] so that \( P_t^{(LCR_i, LCR_{-i})} = 1 \) and thus \( P_t^{(\sigma_i, \sigma_{-i})} \leq P_t^{(LCR_i, LCR_{-i})} \).

Further, \( \tau^{(NSS_i, NSS_{-i})} = \tau^{(NSS_i, LCR_{-i})} = \infty \) a.s. so that \( R < \infty \) yields \( 0 = P_t^{(NSS_i, NSS_{-i})} = P_t^{(NSS_i, LCR_{-i})} < P_t^{(LCR_i, LCR_{-i})} \) as desired. \( \square \)

**Lemma B.1. Stake Lemma**

If \( \min_{i \in I} \pi_i \times S \geq \frac{R}{\log \frac{1}{2}} \) then \( \forall i \in I : \forall (\sigma_i, \sigma_{-i}) \in A_i \times A_{-i} : V_t^{(\sigma_i, \sigma_{-i})} \leq \pi_i S \)

**Proof.**

\[ \forall i \in I : \text{I define } f_i \in C^1([0, \infty)) \text{ such that } f_i(t) = t \log \delta + \log \{Rt + \pi_i S\}. \]

Then, \( \min_{i \in I} \pi_i \times S \geq \frac{R}{\log \frac{1}{2}} \)

implies \( \frac{df_i}{dt} \leq 0 \) so that \( \forall i \in I : \max_{t \geq 0} e^{f_i(t)} = e^{f_i(0)} = \pi_i S. \) Moreover, \( \forall i \in I : \forall (\sigma_i, \sigma_{-i}) \in A_i \times A_{-i} : V_t^{(\sigma_i, \sigma_{-i})} = \sum_{t=0}^{\infty} V_t^{(\sigma_i, \sigma_{-i})} I_{t^{(\sigma_i, \sigma_{-i})}} \leq \sum_{t=0}^{\infty} e^{f_i(t)} I_{t^{(\sigma_i, \sigma_{-i})}} \leq \pi_i S \) \( \square \)

**Proposition 6.2 Immediate Consensus II**

If \( \min_{i \in I} \pi_i \times S \geq \frac{R}{\log \frac{1}{2}} \), then there exists an equilibrium in which each player follows the longest chain rule. In such an equilibrium, the fork resolves at \( t = 0. \)

**Proof.**

\[ \forall i \in I : \tau^{(LCR_i, LCR_{-i})} = 0 \] so that Lemma B.1 implies \( \forall i \in I : \sigma_i \in A_i : V_t^{(\sigma_i, LCR_{-i})} \leq \pi_i S = V_t^{(LCR_i, LCR_{-i})}. \) Then, \( \forall i \in I : \sigma_i \in A_i : \mathbb{E}[V_t^{(\sigma_i, LCR_{-i})}] \leq \mathbb{E}[V_t^{(LCR_i, LCR_{-i})}] \) which completes the proof. \( \square \)
Proposition 6.4 Never Consensus

There exists an equilibrium in which each player follows the Nothing-at-Stake strategy. In such an equilibrium, the fork never resolves with probability one.

Proof.

\[ \forall i \in I : I \text{ define } NSS_{-i} \equiv \bigcap_{j \neq i} NSS_j. \] I proceed by showing that \( \forall i \in I : \sigma_i \in A_i : \tau(\sigma_i, NSS_{-i}) = \infty \) almost surely which implies the desired result.

I define \( Q : I \rightarrow \{1,2\} \) such that \( Q(i) = I_{i \neq 1} + 2I_{i=1}. \) Then, \( \forall i \in I, t \in \mathbb{N} : \forall \sigma_i \in A_i : \{\tau(\sigma_i, NSS_{-i}) \leq t\} \subseteq \bigcup_{b=1}^{2} \bigcap_{s=t+1}^{\infty} \{X_{b,s}^{(\sigma_i, NSS_{-i})} \neq Q(i)\} \) so that \( \forall i \in I, t \in \mathbb{N} : \forall \sigma_i \in A_i : \) \( \mathbb{P}\{\tau(\sigma_i, NSS_{-i}) \leq t\} \leq \sum_{b=1}^{2} \prod_{s=t+1}^{\infty} 1 - \frac{\pi_{Q(i)}S}{S+R_S} \leq \sum_{b=1}^{2} e^{-\frac{\pi_{Q(i)}S}{S+R_S}} = \sum_{b=1}^{2} e^{-\sum_{s=t+1}^{\infty} \frac{\pi_{Q(i)}S}{S+R_S}} = 0. \) Then, \( \forall i \in I : \forall \sigma_i \in A_i : \mathbb{P}\{\tau(\sigma_i, NSS_{-i}) < \infty\} = \lim_{t \to \infty} \mathbb{P}\{\tau(\sigma_i, NSS_{-i}) \leq t\} = 0 \) completes the proof. \( \square \)
C Data Scraping

Blockchain.info provides details for blocks on the Bitcoin blockchain. To reconstruct forks within the blockchain over a certain period of time, I query blockchain.info at every block height added over that time period. To minimize human error, I make these queries from R using the rvest package.

Figure A.1: This figure depicts a screen capture from [https://blockchain.info/block-height/449695](https://blockchain.info/block-height/449695).
Blockchain.info provides rich data regarding the Bitcoin blockchain, but this paper’s purpose requires only a few fields. For a given block, this paper's purpose requires block height, whether that block ended up on the blockchain and the time that the block was appended to a blockchain branch. Figure A.1 provides a screen capture and thereby demonstrates that Blockchain.info provides all three pieces of information. The designation “Orphaned” within the height field indicates that the associated block did not end up on the blockchain whereas the designation “Main chain” indicates that the associated block ended up on the blockchain.