10-1-2019

Bitcoin: An Impossibility Theorem for Proof-of-Work based Protocols

Jacob Leshno

Philipp Strack

BITCOIN: AN IMPOSSIBILITY THEOREM FOR PROOF-OF-WORK BASED PROTOCOLS

By

Jacob Leshno and Philipp Strack

October 2019

Revised November 2019

COWLES FOUNDATION DISCUSSION PAPER NO. 2204R

COWLES FOUNDATION FOR RESEARCH IN ECONOMICS
YALE UNIVERSITY
Box 208281
New Haven, Connecticut 06520-8281

http://cowles.yale.edu/

Bitcoin: An Axiomatic Approach and an Impossibility Theorem

Jacob D. Leshno* Philipp Strack†

October 16, 2019‡

Abstract

Bitcoin's main innovation lies in allowing a decentralized system that relies on anonymous, profit driven miners who can freely join the system. We formalize these properties in three axioms: anonymity of miners, no incentives for miners to consolidate, and no incentive to assuming multiple fake identities. This novel axiomatic formalization allows us to characterize which other protocols are feasible: Every protocol with these properties must have the same reward scheme as Bitcoin. This implies an impossibility result for risk-averse miners: no protocol satisfies the aforementioned constraints simultaneously without giving miners a strict incentive to merge. Furthermore, any protocol either gives up on some degree of decentralization or its reward scheme is equivalent to Bitcoin's.

1 Introduction

In 2008 an unknown person under the pseudonym of Satoshi Nakamoto proposed a protocol to maintain a decentralized currency named bitcoin (Nakamoto, 2008). As of today (October 8, 2019), Bitcoin processes around 350,000 transactions per day, which transfer a total value of approximately 6 Billion US dollar.[1]

Bitcoin's main economic innovation is its decentralized structure: In contrast to traditional systems, no one owns Bitcoin. A fixed protocol governs the rules of the network. The system's infrastructure is provided by anonymous entities who can enter and leave at will, and are free to decide whether or not to follow the rules described by the protocol. Thus, the incentive compatibility of the protocol is crucial for its operation.

This decentralized structure may entail economic benefits, such as the absence of a controlling entity who can extract rents, and the absence of a single point of failure. At the same time,

*University of Chicago, Booth, yarboz@gmail.com. This work is supported by the Robert H. Topel Faculty Research Fund at the University of Chicago Booth School of Business.

†Yale University, Economics Department, philipp.strack@gmail.com

‡An earlier version of this manuscript with the title "Bitcoin: An Impossibility Theorem for Proof-of-Work" was submitted on February 14, 2019 to the EC'19 conference (ACM Conference on Economics and Computation).

[1]Source: https://bitinfocharts.com/bitcoin/

Bitcoin's design has been criticized for its cost and environmental impact.[2] Environmental concerns and other shortcomings of Bitcoin motivated a growing interest among academics and industry in the development of resource-efficient blockchains. Examples of suggestions for alternative designs include proof-of-stake,[3] proof-of-space,[4] and proof-of-replication.[5] Despite these efforts, Bitcoin remains the most popular cryptocurrency.[6]

We employ the methodology commonly used in mechanism design or social choice to understand the limitations of decentralized systems operated by anonymous, selfish agents. We begin by formulating axioms that capture the desired properties and necessary constraints of a decentralized system operated by anonymous, selfish agents. We follow to give characterization of protocols satisfying these axioms (which is akin to the characterization of incentive compatible mechanisms). Our axiomatic approach leads to sharp characterization in the case of risk-neutral miners: Any such protocol must reward a miner proportional to the fraction of computational power he provided to the system. As this is exactly the reward scheme used in the Bitcoin protocol, any protocol must be reward-equivalent to Bitcoin, or violate our axioms. For the case of risk-averse miners we show an impossibility theorem: there does not exist any protocol that is anonymous, robust to merging, and robust to Sybil attacks which leaves miners without incentives to merge.

Our findings show that certain properties of decentralized systems are implied by their underlying economic structure, and thus cannot be solved via cryptographic methods. In order for alternative protocols to provide a different reward scheme these must be able to identify miners (violate anonymity), or restrict the entry of unidentified miners (which allows the protocol to violate robustness to Sybil attacks), or provide the miners with incentives to merge (and therefore limit the decentralization of the system).

Apart from the direct implications for the design of decentralized systems, we view this paper as making a conceptual contribution. The axiomatic approach we utilize allows us to reason about general properties of protocols and analyze necessary economic trade-offs. In particular, a possible economic interpretation of our results is that any protocol must either be equivalent in terms of rewards to Bitcoin or be less decentralized.

[2] Bitcoin is estimated to use at least 53.81 terawatt-hours of power every year, which is roughly equivalent to the power consumption of Switzerland (source: https://www.inverse.com/article/57389-bitcoin-mining-s-incredible-energy-waste-has-been-captured-in-new-research). The network is estimated to cause CO2 emissions of 22.0 to 22.9 MtCO2, which is between the emissions caused by Jordan and Sri Lanka (see Stoll et al., 2019). See also Benetton et al. (2019).

[3] See Gilad et al. (2017), Bentov et al. (2016), Kiayias et al. (2017), and Saleh (2019).

[4] See Dziembowski et al. (2015) and Park et al. (2018).

[5] See Benet et al. (2017).

[6] As of August 2019, there existed more than 1600 digital currencies (source https://en.wikipedia.org/wiki/List_of_cryptocurrencies). Etherum is the second largest cryptocurrency by market capitalization, with a market cap roughly equivalent to 20 Billion USD or 17% of Bitcoin's market cap (source https://coinmarketcap.com/currencies/ethereum/historical-data/).

Related Literature This paper joins a large and growing literature of papers that analyzed miner's incentives to follow Bitcoin's protocol (Eyal and Sirer 2014, Biais et al. 2018, Sapirshtein et al. 2016, Pass et al. 2017, Carlsten et al. 2016, Kiayias et al. 2016), analyzed miners' entry decisions (Prat and Walter 2018, Arnosti and Weinberg 2019), analyzed the implied market for transaction processing (Easley et al. 2017, Huberman et al. 2019, Chiu and Koeppl 2017, Lavi et al. 2019), criticized its resource inefficiency (Budish 2018, Auer 2019), and suggested alternative designs (for example, Chen and Micali 2016, Benet et al. 2017). Most of the literature focuses on analyzing specific protocols, or presents challenges to a general class of protocols (Abadi and Brunnermeier 2018, Brown-Cohen et al. 2019). Our focus is in providing a characterization of protocols that satisfy axiomatic properties. We hope this approach will help elucidate the limitations and trade-offs for any decentralized protocol.[7]

The economic literature also explored other related issues raised by Bitcoin, exploring the question of adoption and competition between different cryptocurrencies (Athey et al. 2016, Halaburda and Sarvary 2016, Gandal and Halaburda 2014, Gans and Halaburda 2015), the valuation of cryptocurrencies and implication for fiscal policy (Schilling and Uhlig 2018, 2019, Fernández-Villaverde and Sanches 2019, Garratt and Wallace 2018, Benigno et al. 2019), and asking whether Bitcoin functions as a currency (Yermack 2013).

Contests where each player wins with a probability equal to her effort divided by total effort have been called Tullock contests in the economic literature. As our axioms imply a functional form that is equivalent to a Tullock contest, our work is distantly related to the literature that proposes axiomatizations of contest success functions (Skaperdas 1996; Clark and Riis 1998). Skaperdas (1996) show that requiring consistency of the winning probabilities in which only a subset of player participates and symmetry with respect to the players implies a functional form that generalizes the Tullok contest. Clark and Riis (1998) generalize this insight to asymmetric contests. The main axiom in both papers states that when a player stops to participate and exerts zero effort the winning probabilities of each other player increases proportionally. While this axiom is very natural in many contexts it is fundamentally different from the axioms we impose that state that there should be no benefit to Sybil attacks or merging.

This note is structured as follows: Section 2 defines a random selection rule based on the number of computations performed by each miner and provides a characterization of all random selection rules that are anonymous and robust to Sybil attacks and merging. Section 3 argues that all three axioms are necessary to obtain the result. We discuss risk-averse miners in section 4. Section 5 shows how existing results for Tullock contests can be used to characterize how many computations miners perform for the network in any decentralized protocol that satisfies our axioms. We conclude in Section 6.

[7] Subsequent to a first version of our paper Chen et al. (2019) also show that the proportional selection rule is the unique selection rule satisfying similar axioms.

2 Random Selection in Decentralized Protocols

Bitcoin's ledger is maintained and updated by a decentralized network of anonymous computers, commonly referred to as miners. A key challenge in the design of the protocol is to maintain consensus (Lamport et al., 1982) among all miners on the ledger (record of accepted transactions) while continuously updating the ledger with new transaction data. Bitcoin achieves this by randomly selecting a single miner that issues an update to the ledger, which is commonly called a "block".

This random selection is carried out through the use of a computational puzzle, without relying on known identities or a trusted randomization device. The Bitcoin protocol asks miners to perform costly computations, whose result is used to determine a single miner to issue the next block. Performing these computations in attempt to issue the next block is commonly referred to as "mining".[8] To incentivize miners to perform these costly computations, Bitcoin rewards miners when they are selected to issue the next block.

We next formalize this random selection of a miner. Let $n \geq 2$, and $N = \{1, \ldots, n\}$ be the set of miners and denote by i a typical miner. Each miner i who takes part in the decentralized system performs a certain amount of computations $x_i \geq 0$, which we refer to as miner i's *contribution*. The probability with which miner i is selected in the Bitcoin protocol equals his computational contribution divided by the total contribution by all miners

$$\frac{x_i}{\sum_{j=1}^{n} x_j}.$$

This selection is achieved by having the miners compute cryptographic hashes. Each computation of a hash is equally likely to lead to a value[9] that allows the miner to write the next block and receive the associated reward.[10]

The selection rule is a critical ingredient of any decentralized protocol, as it determines the incentives of miners to contribute to the system. Abstracting away from computational aspects of the problem, we define a random selection rule as follows:

Definition 1 (Selection Rule)**.** *A random selection rule p is described by a family of functions $p^n : \mathbb{R}^n_+ \to \Delta^n$ indexed by $n \in \mathbb{N}$ such that the probability with which miner $i \in N$ is selected at the contribution profile $x = (x_1, \ldots, x_n)$ equals*

$$p_i^n(x_1, \ldots, x_n),$$

which is non-decreasing in x_i.

[8] While miners need to perform other computational tasks (such as validating transactions, storing the ledger, etc.), the vast majority of the miner's computational resources is spent on mining (Croman et al., 2016).

[9] The target value is adjusted periodically, so that on average a single miner is selected to issue a new block every ten minutes.

[10] Under standard cryptographic assumptions, there is no computational method for finding a valid solution that is more efficient than simply attempting many hashes.

Computational contributions induced by proportional and WTA selection Different selection rules can lead to very different outcomes. To illustrate this, consider a situation with n miners and compare two selection rules: The first one is the proportional selection rule used by Bitcoin.

Definition 2 (Proportional Selection Rule)**.** *In the proportional selection rule miners are selected with probability proportional to their contribution*

$$p_i^n(x_1, \ldots, x_n) = \frac{x_i}{\sum_{i=1}^n x_j}$$

In the second rule the miner who contributed the most always wins.

Definition 3 (Winner-Take-All Rule)**.** *In the winner-take-all rule the miner who contributed the most wins and ties are broken randomly*

$$p_i^n(x_1, \ldots, x_n) = \begin{cases} \frac{1}{|\{i\colon x_i = \max_{j\in N} x_j\}|} & \text{if } x_i = \max_{j\in N} x_j \\ 0 & \text{else} \end{cases}.$$

To illustrate the different behaviour induced by these selection rules, assume for the example that each miner's marginal cost of performing computations equals 1 and that the reward when mining a block equals 1. It is easily seen that under the proportional selection rule there is a unique Nash equilibrium where each miner contributes[11]

$$x_i = \frac{n-1}{n^2}.$$

In contrast, under the winner-take-all (WTA) rule there is a unique symmetric Nash equilibrium where each miner randomizes his contribution on $[0, 1]$ according to[12]

$$\mathbb{P}[x_i \leq s] = \sqrt[n-1]{s}.$$

These two equilibrium outcomes resulting from different selection rules differ across several dimensions. For example, under the proportional rule miners follow a simple pure strategy in equilibrium, while under the WTA rule there are no pure strategy equilibrium and miners must randomize. Furthermore, the expected equilibrium contributions differ between the two selection rules.

A Mechanism Design Perspective We are interested in which selection rules can be used to maintain a decentralized system. In terms of the miners' behaviour the two above selection rules

[11] We argue this formally in Section 5.

[12] This follows from the strategic equivalence between this game and the complete information all-pay auction, and the characterization of all-pay auction equilibria given in Barut and Kovenock (1998).

are equivalent to using a Tullok contest or an all-pay-auction for allocating the next block to a miner. The question of designing an optimal selection rule is similar to the classical mechanism design question of allocating a single object among several bidders using transfers. In the single object allocation problem a mechanism specifies the probability with which each bidder gets the object and the transfer made by each bidder as a function of the valuations of bidders. Similarly, a selection rule determines the probabilities with which miners are selected and their computational contributions (which are the analogue of transfers). As in the classical mechanism design approach we start by characterizing selection rules which satisfy certain incentive constraints following from the decentralized nature of the protocol (the analog of incentive compatible mechanisms). This characterization of "feasible selection rules" is a necessary first step to finding the optimal selection rule according to some criterion. What differs between our problem and the classical mechanism design context are the restrictions imposed on selection rules: The requirement that the protocol should operate in a decentralized manner imposes additional restrictions not present in the mechanism design context. The next section presents axioms that formalize these restrictions.

2.1 Three Axioms for Decentralized Protocols

The first constraint we impose is anonymity. It states that every miner is treated the same by the mechanism: If two miners exchange their identities their outcomes remain unchanged. For example in the Bitcoin protocol all miners are treated the same as they all face the same requirement to be selected to mine the next block.

Axiom 1 (Anonymity)**.** *A selection rule is anonymous if it is invariant under permutations, i.e. for every n and every permutation $\pi : \mathbb{R}^n_+ \to \mathbb{R}^n_+$ it satisfies $\pi(p^n(x)) = p^n(\pi(x))$.*

Anonymity is a key features of a decentralized system which aims to attract anonymous agents to freely join the system. Note that this anonymity axiom is strong in that it does not allow the protocol to treat agents differently based on the agents' history within the system (as would be the case in some proof-of-stake protocols). Allowing dependence on the agent's history can give incumbents an advantage over new entrants, hindering free entry of miners.

Our next axiom ensures that no miner can increase his winning probability without increasing his contribution by posing as a new entrant, and splitting its computations between the two identities.

Axiom 2 (Robustness to Sybil Attacks)**.** *An selection rule is robust to Sybil attacks if for every $x \in \mathbb{R}^n_+, i \in N$ and every $\Delta \in [0, x_i]$*

$$p_i^n\big(x\big) \geq p_i^{n+1}\big(y\big) + p_{n+1}^{n+1}\big(y\big)\,,$$

where $y = \big(x_1, \ldots, x_{i-1}, x_i - \Delta, x_{i+1}, \ldots, x_n, \Delta\big)$.

Axiom 2 implicitly encodes a free entry condition: Whenever only n miners are present in the system, a new miner can join and claim the role of miner $n+1$.[13] In a decentralized setting without verifiable identities, an existing participant can also assume the role of a new entrant. Axiom 2 formalizes the implied incentive constraint that is present in a protocol with free entry and no verifiable identities.[14]

Axiom 3 (Robust to Merging)**.** *An random selection rule is robust to merging if for every* $x \in \mathbb{R}^n_+$ *and every* $i, j \in N$

$$p_i^n(x) + p_j^n(x) \geq p_i^n(y) + p_j^n(y)\,,$$

where $y = (x_1, \ldots, x_{i-1}, x_i + x_j, x_{i+1}, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n)$.

Robustness to merging imposes a decentralization requirement: No two miners can merge and increase their joint winning probability. A mechanism which is not robust to merging will, by definition, provide some miners with incentives to merge. This might lead such a selection mechanism to be, in the long-run, controlled by relatively few miners.

Centralization is undesirable for cryptocurrencies, as it undermines the security of the decentralized system. Nakamoto (2008) argues that Bitcoin is secure as long as no party controls more than 50% of the computational power. Subsequent research analysed whether Bitcoin is susceptible to various types of attacks by miners under differing assumptions. The main common finding in this literature is that the integrity of the network can be preserved as long as no miner performs more than a certain fraction of the computations. This fraction varies depending on assumptions and considered attacks between 33% and 50%.[15]

Our main result characterizes all selection rules satisfying these decentralization properties:

Theorem 1. *A random selection rule* p *is anonymous, robust to Sybil attacks, and robust to merging if and only if is the proportional selection rule*

$$p_i^n(x) = \frac{x_i}{\sum_{j=1}^n x_j}\,. \tag{1}$$

Equation 1 states that the probability with which an miner is selected is proportional to the share of computations she performed. For example, it describes the probability that a miner is selected to mine the next block in Bitcoin: Miners attempt to mine the next Bitcoin block once

[13] On its own, this free entry condition imposes almost no restriction as miner $n+1$ can be excluded by always assigning him a winning probability of zero. However, in conjunction with anonymity the possibility of free entry imposes further restrictions as a new entrant has to be treated like the miners already present in the system.

[14] While the possibility of free entry imposes constraints, it also creates benefits for the protocol: Huberman et al. (2019) shows that free entry in Bitcoin prevents all miners, including large miners, from profitably affecting transaction fees. But if entry of new miners is blocked, large miners can gain by increasing transaction fees. Prat and Walter (2018) analyzes miner entry decision in a dynamic setting where entry requires an fixed upfront investment in hardware. While there may be no entry in some periods, hardware obsolescence gives rise to an ongoing stream of entrants.

[15] See for example Sompolinsky and Zohar (2015), Pass et al. 2017, Biais et al. 2018, Eyal and Sirer 2018.

the previous block was published (we abstract from some technical details and assume blocks are transmitted instantaneously to all miners) by attempting different values of a nonce and computing their hashes. Under common cryptographic assumptions, no miner can do better than guess a random nonce and each nonce entails the same probability of being selected (to mine the next block). Thus, the probability with which an miner is selected in the Bitcoin protocol equals the number of hashes she computed relative to the total number of hashes computed before the next block is mined.

The proof of Theorem 1 shows that the monotonicity of the selection rule is not necessary if one restricts attention to the case where investments are rational numbers. In any practical application where quantities invested can be finitely encoded the restriction to rational number is vacuously satisfied and thus the monotonicity assumption plays no role.

3 Necessity of the Axioms

Anonymity To see that anonymity is necessary to our characterization to hold, observe that given $q \in (0,1)$ the selection rule

$$p_i^n(x) = \begin{cases} 0 & \text{if } i \notin \{1,2\} \\ q & \text{if } i = 1 \\ 1-q & \text{if } i = 2 \end{cases}.$$

satisfies robustness to Sybil attacks and robustness to merging, but violates the anonymity axiom as it treats miner 1 and 2 different from everybody else. In this selection rule only miner 1 and 2 can win a block.

Robustness to Sybil attacks Next, we show that the robustness to Sybil attacks is necessary for our characterization to hold. Consider for example the selection rule

$$p_i^n(x) = \frac{1}{n}$$

which selects one miner uniformly at random, independently of their contribution. This selection rule is anonymous and robust to merging. It also does not requires miners to perform any costly computations.[16] This rule is clearly not robust to Sybil attacks, as a miner who poses as a group of independent miners increases his chances of being selected.

[16]Such a selection rule is desirable in a context, like Bitcoin, where the main goal of the protocol is to ensure randomness of the selection and the computations performed as part of the protocol are wasteful.

Robustness to Merging Consider the winner-take-all rule (definition 3). This rule is anonymous and robust to Sybil attacks, but not robust to merging. To see this note that if two miners merge they still win whenever one (or both) of them would have won, but in addition also win whenever the sum of the contributions exceeds the maximal contribution.

4 Risk-Averse Miners

So far we have been agnostic about the risk attitudes of miners. Axiom 3 presents a weak requirement that is necessary for risk-neutral miners not to have incentives to merge. However, if miners are risk-averse their incentives to merge increase and Axiom 3 is not sufficient to ensure that miners do not want to merge.

Consider any protocol that is anonymous, robust to Sybil attacks and merging (i.e. satisfies Axiom 1-3). By Theorem 1 such a protocol induces a proportional selection rule. Suppose that in such a selection rule miners i and j who are winning with probability p_i and p_j merge and split the price in case they win according to their relative contributions. Together, they now win with probability p_i+p_j. If they win miner i receives a share of $\frac{x_i}{x_i+x_j}$ of the reward from mining the block and miner j receives a share of $\frac{x_j}{x_i+x_j}$. The reward given to either miner in this sharing scheme equals exactly the expected reward of that miner conditional on either i or j winning the block before merging. The original lottery over rewards when not merging is thus a mean preserving spread of the lottery faced by a miner when merging. Hence, it is strictly better for the two miners to merge whenever they are risk-averse. This argument leads to the following corollary:

Corollary 1. *For every selection rule that satisfies Axiom 1-3 any two risk averse miners have a strict incentive to merge their computational contributions and share the reward from mining a block proportional to their respective contributions.*

An economic implication of Corollary 1 is that large mining pools, where miners pool their resources[17] can not be avoided in any decentralized protocol when miners are sufficiently risk-averse. Corollary 1 thus suggests that risk aversion of the miners is an impediment to the decentralization of the network.

5 Equilibrium Contributions

We next endogenize the computing power x_i contributed by each miner i to the system. This section does not produce any novel results, but illustrates the power of our main result. As by Theorem 1 it suffices to understand Tullock contests to reason about the computational contributions in any decentralized protocol we can leverage known results about Tullock contests to better understand

[17]For analysis of mining pools see Fisch et al. (2017), Cong et al. (2019), and Schrijvers et al. (2016).

decentralized protocols. Prior to our work Arnosti and Weinberg (2019) studied these implication for the special case of Bitcoin and our Theorem 1 implies that their analysis generalizes to arbitrary proof-of-work protocols.[18]

Each miner i pays a cost of $c_i : \mathbb{R}_+ \to \mathbb{R}_+$ depending on how many computations she performs. Throughout, we assume that c_i is strictly increasing, with $c_i(0) = 0$. The later assumption ensures that each miner i participates in the system voluntarily, and we use $x_i = 0$ to denote that the miner did not enter (and receives a zero payoff).[19]

As we have shown in Theorem 1 the total payoff of miner i in every decentralized, anonymous protocol that is robust to Sybil attacks as a function of the computations performed by every participant is thus given by

$$p_i^n(x_1, \ldots, x_n) - c_i(x_i) = \frac{x_i}{\sum_{j=1}^n x_j} - c_i(x_i)\,. \tag{2}$$

The functional form of the payoff (2) is well known in the economics literature as a Tullock contest (Tullock et al., 1980). Each miner maximizes her payoff and we thus look for Nash equilibria of the game. Szidarovszky and Okuguchi (1997) show that if all miners have convex, twice differentiable cost functions there exists a unique pure strategy Nash equilibrium. To describe the equilibrium it is helpful to denote the total computational power in the system by $s = \sum_{i=1}^n x_i$. We denote by $\rho_i(s)$ the unique solution to the equation

$$s^2 c_i'(\rho_i(s)) = s - \rho_i(s)$$

if $sc_i'(0) < 1$ and set $\rho_i(s) = 0$ otherwise. Intuitively, the function $\rho_i(s)$ describes the best-response of miner i if the total computational power of the system equals s.

The next result follows immediately from combining Szidarovszky and Okuguchi (1997) with our Theorem 1:

Corollary 2. *Consider an arbitrary decentralized, anonymous protocol that is robust to Sybil attacks. Suppose that the cost of computation is strictly convex and twice differentiable. There exists a unique pure strategy Nash equilibrium. The total computational power of the system $s = \sum_{i=1}^n x_i$ in equilibrium is solves*

$$s = \sum_{i=1}^n \rho_i(s)$$

and the number of computations performed by miner i equals $\rho_i(s)$

[18] Arnosti and Weinberg (2019) already farsightedly discuss in their conclusion that it might be difficult for another protocol to achieve more decentralization than Bitcoin if there is a risk of Sybil attacks: "Ideally, a miner's expected return would be concave in their share of mining power. This seems difficult to achieve in practice, as miners can always divide their hardware among several false identities."

[19] We can simplify notation this way as any miner who performs no computations never wins by Theorem 1.

If the contestants costs are linear $c_i(x_i) = \beta_i x_i$ it was previously established in Hillman and Riley (1989) that the same characterization holds, but can be further simplified. Without loss assume that $\beta_1 \leq \beta_2 \leq \ldots \leq \beta_n$ and denote by

$$m = \min \left\{ k \colon \beta_{k+1} \geq \frac{k}{k-1} \operatorname{avg}(\beta_1, \ldots, \beta_k) \right\} \tag{3}$$

the first miner m whose follower's marginal cost is greater than $\frac{m}{m-1}$ times the average of the marginal cost of miners with lower marginal cost. In equilibrium only miners 1 to m will chose to enter and perform compuations.

Corollary 3. *Consider an arbitrary decentralized, anonymous protocol that is robust to Sybil attacks. Assume that $c_i(x_i) = \beta_i x_i$ and let m solve (3). The total computational power of the system equals*

$$s = \frac{m-1}{m} \frac{1}{\operatorname{avg}(\beta_1, \ldots, \beta_m)}$$

and the number of computations performed by miner i is given by

$$x_i = \begin{cases} 0 & \text{if } i > m \\ s(1 - \beta_i s) & \text{if } i \leq m \end{cases}. \tag{4}$$

Again this result follows immediately from the combination of our Theorem 1 and Hillman and Riley (1989). Rearranging (4) for the winning probability x_i/s yields immediately that a participating miner is chosen with probability

$$1 - \beta_i s = 1 - \frac{\beta_i (m-1)}{\sum_{j=1^n} \beta_j}.$$

To illustrate these results we provide a simple example:

Example 1 Consider a situation where there are two miners providing computational power to the system. Assume main cost factor are energy cost which are roughly linear in the number of computations performed. miner 1's energy cost are $\gamma\beta$ while miner 2's energy cost equal β, i.e. $c_1(x_1) = \gamma\,\beta\,x_1$ and $c_2(x_2) = \beta\,x_2$. In this case $m = 2$ and miner 1 wins with probability $\frac{1}{\gamma+1}$. Thus, the winning probability of miner 1 depends only on the ratio between her marginal cost and miner 2's marginal cost. For example if miner 1 faces twice as high energy cost she performs only $1/3$ of the computations. This, illustrates that a concentration towards those participants with low energy cost is unavoidable in *any* protocol satisfying our axioms. Any protocol that avoids such a dependence on computational cost has to give up either on anonymity, robustness to merging or robustness to Sybil attacks.

6 Conclusion

The introduction of Bitcoin was followed by much popular interest and excitement about the potential of decentralized protocols. This paper takes a step towards understanding the novel economic systems that can or cannot be enabled by this technology.

One notable example of a design approach that violates our assumption is Proof-of-Stake, in which miners are identified based on their previous actions within the platform (for example, posting a required collateral), violating our strong anonymity axiom. While such design may have numerous advantageous, our axioms capture desiderata for decentralized systems that that such designs will satisfy. In particular, such systems do not satisfy the strong notion of free-entry that motivates our axioms. We hope that our results and following axiomatic work will be helpful in clarifying the trade-offs in design decentralized systems.

Finally, our analysis abstracts from the details of the computations used to perform the random selection. While our results do not rely on computational details, we note that the choice of computational tasks may have several economically important implications. (i) A change to the computational tasks used may change the cost functions of miners. In particular, the availability of fixed cost investment that reduces the cost of the computation task[20] can affect entry dynamics. (ii) Different computational tasks may induce miners to exert different unpriced externalities. For example, different computational tasks may induce miner to spend their budget on storage capabilities rather than electricity consumption (for example, Dziembowski et al. 2015), which may result in a lower environmental impact.

References

Abadi, J. and Brunnermeier, M. (2018). Blockchain economics. Technical report, mimeo Princeton University.

Arnosti, N. and Weinberg, S. M. (2019). Bitcoin: A natural oligopoly. In *Proceedings of ITCS 2019*.

Athey, S., Parashkevov, I., Sarukkai, V., and Xia, J. (2016). Bitcoin pricing, adoption, and usage: Theory and evidence.

Auer, R. (2019). Beyond the doomsday economics of "proof-of-work" in cryptocurrencies.

Barut, Y. and Kovenock, D. (1998). The symmetric multiple prize all-pay auction with complete information. *European Journal of Political Economy*, 14(4):627–644.

Benet, J., Dalrymple, D., and Greco, N. (2017). Proof of replication. *Protocol Labs, July*, 27.

[20] Prat and Walter (2018) discusses the effect of dedicated hardware on miner entry dynamics.

Benetton, M., Compiani, G., and Morse, A. (2019). Cryptomining: Energy use and local impact.

Benigno, P., Schilling, L. M., and Uhlig, H. (2019). Cryptocurrencies, currency competition, and the impossible trinity. Technical report, National Bureau of Economic Research.

Bentov, I., Pass, R., and Shi, E. (2016). Snow white: Provably secure proofs of stake.

Biais, B., Bisiere, C., Bouvard, M., and Casamatta, C. (2018). The blockchain folk theorem.

Brown-Cohen, J., Narayanan, A., Psomas, A., and Weinberg, S. M. (2019). Formal barriers to longest-chain proof-of-stake protocols. In *Proceedings of the 2019 ACM Conference on Economics and Computation*, pages 459–473. ACM.

Budish, E. (2018). The economic limits of bitcoin and the blockchain. Technical report, National Bureau of Economic Research.

Carlsten, M., Kalodner, H., Weinberg, S. M., and Narayanan, A. (2016). On the instability of bitcoin without the block reward. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 154–167. ACM.

Chen, J. and Micali, S. (2016). Algorand. *arXiv preprint arXiv:1607.01341*.

Chen, X., Papadimitriou, C., and Roughgarden, T. (2019). An axiomatic approach to block rewards. *arXiv preprint arXiv:1909.10645*.

Chiu, J. and Koeppl, T. (2017). The economics of cryptocurrencies–bitcoin and beyond.

Clark, D. J. and Riis, C. (1998). Contest success functions: an extension. *Economic Theory*, 11(1):201–204.

Cong, L. W., He, Z., and Li, J. (2019). Decentralized mining in centralized pools. Technical report, National Bureau of Economic Research.

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

Dziembowski, S., Faust, S., Kolmogorov, V., and Pietrzak, K. (2015). Proofs of space. In *Annual Cryptology Conference*, pages 585–605. Springer.

Easley, D., O'hara, M., and Basu, S. (2017). From mining to markets: The evolution of bitcoin transaction fees. *Working paper*.

Eyal, I. and Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In *International Conference on Financial Cryptography and Data Security*, pages 436–454. Springer.

Eyal, I. and Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, 61(7):95–102.

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

Fisch, B., Pass, R., and Shelat, A. (2017). Socially optimal mining pools. In *International Conference on Web and Internet Economics*, pages 205–218. Springer.

Gandal, N. and Halaburda, H. (2014). Competition in the cryptocurrency market.

Gans, J. S. and Halaburda, H. (2015). Some economics of private digital currency. In *Economic Analysis of the Digital Economy*, pages 257–276. University of Chicago Press.

Garratt, R. and Wallace, N. (2018). Bitcoin 1, bitcoin 2,....: An experiment in privately issued outside monies. *Economic Inquiry*, 56(3):1887–1897.

Gilad, Y., Hemo, R., Micali, S., Vlachos, G., and Zeldovich, N. (2017). Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles*, pages 51–68. ACM.

Halaburda, H. and Sarvary, M. (2016). Beyond bitcoin. *The Economics of Digital Currencies*.

Hillman, A. L. and Riley, J. G. (1989). Politically contestable rents and transfers. *Economics & Politics*, 1(1):17–39.

Huberman, G., Leshno, J., and Moallemi, C. C. (2019). An economic analysis of the bitcoin payment system. *Columbia Business School Research Paper*, (17-92).

Kiayias, A., Koutsoupias, E., Kyropoulou, M., and Tselekounis, Y. (2016). Blockchain mining games. In *Proceedings of the 2016 ACM Conference on Economics and Computation*, pages 365–382. ACM.

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

Lamport, L., Shostak, R., and Pease, M. (1982). The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401.

Lavi, R., Sattath, O., and Zohar, A. (2019). Redesigning bitcoin's fee market. In *The World Wide Web Conference*, pages 2950–2956. ACM.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Park, S., Kwon, A., Fuchsbauer, G., Gaži, P., Alwen, J., and Pietrzak, K. (2018). Spacemint: A cryptocurrency based on proofs of space. In *International Conference on Financial Cryptography and Data Security*, pages 480–499. Springer.

Pass, R., Seeman, L., and Shelat, A. (2017). Analysis of the blockchain protocol in asynchronous networks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 643–673. Springer.

Prat, J. and Walter, B. (2018). An equilibrium model of the market for bitcoin mining.

Saleh, F. (2019). Blockchain without waste: Proof-of-stake. *Available at SSRN 3183935*.

Sapirshtein, A., Sompolinsky, Y., and Zohar, A. (2016). Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 515–532. Springer.

Schilling, L. and Uhlig, H. (2018). Some simple bitcoin economics. Technical report, National Bureau of Economic Research.

Schilling, L. M. and Uhlig, H. (2019). Currency substitution under transaction costs. In *AEA Papers and Proceedings*, volume 109, pages 83–87.

Schrijvers, O., Bonneau, J., Boneh, D., and Roughgarden, T. (2016). Incentive compatibility of bitcoin mining pool reward functions. In *International Conference on Financial Cryptography and Data Security*, pages 477–498. Springer.

Skaperdas, S. (1996). Contest success functions. *Economic theory*, 7(2):283–290.

Sompolinsky, Y. and Zohar, A. (2015). Secure high-rate transaction processing in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 507–527. Springer.

Stoll, C., Klaaßen, L., and Gallersdörfer, U. (2019). The carbon footprint of bitcoin. *Joule*.

Szidarovszky, F. and Okuguchi, K. (1997). On the existence and uniqueness of pure nash equilibrium in rent-seeking games. *Games and Economic Behavior*, 18(1):135–140.

Tullock, G., Buchanan, J. M., and Tollison, R. D. (1980). Toward a theory of the rent-seeking society. *Efficient rent seeking*, 97:112.

Yermack, D. (2013). Is bitcoin a real currency? an economic appraisal. Technical report, National Bureau of Economic Research.

A Proofs

Lemma 1. *Consider a selection rule that is robust to Sybil attacks. For every $x \in \mathbb{R}_+^n$ and every $y \in \mathbb{R}_+^k$ with $\sum_{j=1}^k y_j = x_n$*

$$p_n^n(x_1, \dots, x_n) \geq \sum_{j=n}^{n+k-1} p_j^{n+k-1}(x_1, x_2, \dots, x_{n-1}, y_1, \dots, y_k)\,.$$

Proof. The result follows by sequentially applying the robustness to Sybil attacks to miner $r \in \{n, \dots, n+k-2\}$ with $\Delta_r = \sum_{j=r+1}^{n+k-1} y_j$. □

Lemma 2. *We have that for all $i \in \{1, \dots, n\}$*

$$p_i^n(x_1, \dots, x_n) = p_i^{n+1}(x_1, \dots, x_n, 0)\,,$$

and $p_{n+1}^{n+1}(x_1, \dots, x_n, 0) = 0$.

Proof. The robustness to Sybil attacks by Lemma 1 implies that for each agent i

$$p_i^n(x_1, \dots, x_n) \geq p_i^{n+1}(x_1, \dots, x_n, 0) + p_{n+1}^{n+1}(x_1, \dots, x_n, 0)\,.$$

Summing up over all agents $i \in \{1, \dots, n\}$ yields

$$\begin{aligned} 1 &\geq \left(\sum_{i=1}^n p_i^{n+1}(x_1, \dots, x_n, 0)\right) + n\, p_{n+1}^{n+1}(x_1, \dots, x_n, 0) = 1 + (n-1) p_{n+1}^{n+1}(x_1, \dots, x_n, 0) \\ \Rightarrow 0 &= p_{n+1}^{n+1}(x_1, \dots, x_n, 0)\,. \end{aligned}$$

Where we used in the first equality that the combined winning probability of all miners equals 1 and in the second equality that winning probabilities are non-negative.

We thus have that $p_i^n(x_1, \dots, x_n) \geq p_i^{n+1}(x_1, \dots, x_n, 0)$ for all agents $i \in \{1, \dots, n\}$. As winning probabilities sum up to 1 we get that

$$p_i^n(x_1, \dots, x_n, 0) = 1 - \sum_{j \neq i} p_j^{n+1}(x_1, \dots, x_n, 0) \leq 1 - \sum_{j \neq i} p_j^n(x_1, \dots, x_n) = p_i^n(x_1, \dots, x_n)\,.$$

This establishes the lemma. □

Lemma 3. *In any selection rule that is robust to merging we have that for every $x \in \mathbb{R}_+^n$ and every $y \in \mathbb{R}_+^k$ with $\sum_{j=1}^k y_j = x_n$*

$$p_n^n(x_1, \dots, x_n) \leq \sum_{j=n}^{n+k-1} p_j^{n+k-1}(x_1, x_2, \dots, x_{n-1}, y_1, \dots, y_k)\,.$$

Proof. Applying the condition for robustness to merging sequentially agent by agent yields that

$$p_n^{n+k-1}\big(x_1,\dots,x_n,0,\dots,0\big) \leq \sum_{j=n}^{n+k-1} p_j^{n+k-1}\big(x_1,x_2,\dots,x_{n-1},y_1,\dots,y_k\big)\,.$$

Applying Lemma 2 iteratively for agent $j \in \{n+1,\dots,n+k-1\}$ yields that

$$p_n^{n+k-1}\big(x_1,\dots,x_n,0,\dots,0\big) = p_n^n\big(x_1,\dots,x_n\big)$$

and thus the result follows. □

Corollary 4. *Consider a selection rule that is robust to merging and to Sybil attacks. For every $x \in \mathbb{R}_+^n$ and every $y \in \mathbb{R}_+^k$ with $\sum_{j=1}^k y_j = x_n$*

$$p_n^n\big(x_1,\dots,x_n\big) = \sum_{j=n}^{n+k-1} p_j^{n+k-1}\big(x_1,x_2,\dots,x_{n-1},y_1,\dots,y_k\big)\,.$$

Proof. Follows immediately from Lemma 1 and Lemma 3. □

Proof of Theorem 1. We begin by showing the axioms imply the functional form (1) in the case where the investment of each miner is rational $x \in \mathbb{Q}_+^n$. Consider an arbitrary vector of investments $x \in \mathbb{Q}_+^n$ and w.l.o.g assume that all investments are expressed with respect to a common denominator $b \in \mathbb{N}$, i.e. there exists $a \in \mathbb{N}^n$ such that $x_i = {}^{a_i}\!/_b$. We begin by splitting the first miner into a_1 miners each of which makes an investment of ${}^1\!/_b$. As a consequence of Corollary 4 and the anonymity it follows that the joint winning probability of the first a_1 miners after this split equals the original winning probability of the first miner

$$p_1^n(x) = \sum_{j=1}^{a_1} p_j^{n+a_1-1}\left(\frac{1}{b},\dots,\frac{1}{b},\frac{a_2}{b},\dots,\frac{a_n}{b}\right)\,.$$

In the next step we merge the last $n-1$ miners into a single miner. Again by Corollary 4 the winning probability of the last miner in the new situation equals the joint winning probability of the last $n-1$ miners in the old situation. As the winning probabilities sum up to 1 the joint winning probability of the first a_1 miners remains unaffected and we have that

$$p_1^n(x) = \sum_{j=1}^{a_1} p_j^{a_1+1}\left(\frac{1}{b},\dots,\frac{1}{b},\frac{\sum_{i=2}^n a_i}{b}\right)\,.$$

In the next step we split the a_1+1 miner into $\sum_{i=1}^n a_i$ miners each investing $\frac{1}{b}$. Again, by Corollary

4 this implies that

$$p_1^n(x) = \sum_{j=1}^{a_1} p_j^{|a|}\left(\frac{1}{b},\dots,\frac{1}{b}\right),$$

where $|a| = \sum_{i=1}^n a_i$. It follows from anonymity that each of the miners wins with equal probability of $1/|a|$, and thus

$$p_1^n(x) = \frac{a_1}{|a|} = \frac{a_1/b}{|a|/b} = \frac{x_1}{\sum_{j=1}^n x_j}.$$

To extend this result from $\mathbb{Q}_+^n$ to $\mathbb{R}_+^n$ we first show that the result extends to vectors where the first coordinate is chosen from $\mathbb{R}_+$ instead of $\mathbb{Q}_+$. Consider an arbitrary $x_{-1} \in \mathbb{Q}_+^{n-1}$ and $x_1 \in \mathbb{R}_+$. Choose two sequences $w^r, v^r \in \mathbb{Q}_+$ such that w^r converges to x_1 from above and v^r converges to x_1 from below when $r \to \infty$. By monotonicity we have that

$$\frac{v^r}{v^r + \sum_{j=2}^n x_j} \le p_1^n(x_1, x_{-1}) \le \frac{w^r}{w^r + \sum_{j=2}^n x_j}.$$

As the lower bound and the upper bound converge to the same limit it follows that $p_1^n(x) = \frac{x_1}{|x|}$ for all x with $x_1 \in \mathbb{R}_+$ and $x_{-1} \in \mathbb{Q}_+^{n-1}$. By anonymity $p_2^2(x) = \frac{x_2}{|x|}$ for all x with $x_{-2} \in \mathbb{Q}_+^{n-1}$ and $x_2 \in \mathbb{R}_+$. Thus, for $x_{-2} \in \mathbb{Q}_+^{n-1}$ and $x_2 \in \mathbb{R}_+$ we have that

$$p_1^n(x) = 1 - p_2^n(x) - \sum_{k=3}^n p_k^n(x) = 1 - \frac{x_2}{|x|} - \sum_{k=3}^n \frac{x_k}{|x|} = \frac{x_1}{|x|}.$$

Applying the above argument with an upper and lower bound again yields that for all x with $(x_1, x_2) \in \mathbb{R}_+^2$ and $(x_3, \dots, x_n) \in \mathbb{Q}_+^{n-2}$ we have that $p_1^n(x) = \frac{x_1}{|x|}$. Applying the same argument sequentially for each miner $k \ge 3$ yields that $p_1^n(x) = \frac{x_1}{|x|}$ for all $x \in \mathbb{R}_+^n$. By permuting the role of miner 1 and miner i and anonymity we have that $p_i^n(x) = \frac{x_i}{\sum_{j=1}^n x_j}$ for all $i \in \{1, .., n\}$ and all $x \in \mathbb{R}_+^n$.

We are left to verify that the functional form (1) satisfies our assumptions. Clearly (1) is monotonic and anonymous. Furthermore, we have that for every $y \in \mathbb{R}_+^k$ with $|y| = x_1$

$$\sum_{j=1}^k p_j^{n+k-1}(y_1, \dots, y_k, x_2, x_3, \dots, x_n) = \sum_{j=1}^k \frac{y_j}{|y| + \sum_{i=2}^n x_i} = \frac{x_1}{\sum_{i=1}^n x_i} = p_1^n(x),$$

which shows that the functional form (1) is robust to Sybil attacks and merging and completes the proof. □