Allocating rights to mine blocks

Mitri Kitti*

Department of Economics, University of Turku, FI-20014, Finland

Abstract

This paper studies mechanisms for allocating rights to forge new blocks on a blockchain. The proof of work contest (PoW) where all block generators, or miners, compete for finding the next block is characterized. The central feature of the PoW contest is that no miner has an incentive to participate with multiple identities—a property called sybil proofness. There are several alternatives for the PoW that involve payments and messaging between the miners and the protocol, features that are not used in the PoW contest. A class of mechanisms that generalizes the proof of stake procedure is introduced for allocating multiple rights to carry out the mining of blocks. These mechanisms are characterized by a set of elementary properties. Auctioning the rights to add blocks into a blockchain is also considered.

Keywords: mechanism design, blockchain, auction, contest, proof of work, proof of stake, sybil proof, mining
JEL: D82, D44, C72, D74, L86, G2

1. Introduction

A blockchain is a distributed ledger that can be used in recording events such as transactions, in a secure and a verifiable way such that the records are practically impossible to alter once stored in the ledger. The blockchain technology has raised a lot of attention and some argue that it has the potential to create new foundations for our economic and social systems (Iansati and Lakhami, 2017), and disrupt prevailing monetary arrangements (Böhme et al., 2015). This far, the main applications of the technology are various cryptocurrencies, most notably Bitcoin (Nakamoto, 2008), which has a current market capitalization of about 120 billion dollars, see Cheah and Fry (2015); Ciain et al. (2016); Li and Wang (2017) on the determination of the value of Bitcoin.

*Email: mitri.kitti@gmail.com

A central element of any blockchain technology is the process of adding or forging new blocks on the blockchain. In many cases this process is tied to the way how the consensus on the contents of the ledger is achieved. However, as done in this work, allocating the rights to forge new blocks can be separated from the forming of consensus, although the way how consensus is reached may affect the incentives of forging new blocks.

The proof of work (PoW) is the most widely adopted consensus mechanism among various blockchain based cryptocurrencies. This mechanism relies on a common protocol that accepts one blockchain over another if it is harder to generate. Moreover, the PoW based protocols typically allow anyone to participate in the contest of forging new blocks: the one who finds the new block first is rewarded. However, there are other mechanism both for achieving the consensus and allocating rights to forge new blocks. One alternative is the proof of stake mechanism, where the right to forge a block is given randomly to a single miner such that the probability of getting selected depends on the cost paid by the participants of the mechanism. For the theory of the proof of work as a consensus mechanism see Saleh (2017).

How the forging of new blocks is arranged affects all the decision makers involved in the use of the blockchain but even to third parties. First and foremost, the choice of blockchain mining arrangements; who has the permission to forge blocks and how the miners are rewarded, is a major decision with long lasting consequences to the security, adoption, and transaction costs. In particular, the security properties and transaction costs have implications for the conduct of e-commerce with cryptocurrencies, see Polasik et al. (2015) on the adoption of Bitcoin in online payments.

Since adding blocks is computationally extremely demanding and requires significant amounts of energy, blockchain technologies may cause considerable negative externalities. O'Dwyer and Malone (2014) estimate that the yearly energy usage of Bitcoin mining is comparable to that of Ireland. Hence, the security of the public ledger comes at the cost of massive welfare loss in terms of wasted energy. Consequently, there is a need for mechanisms that can be used to reach a balance between the security of a blockchain and the effort for maintaining it. This issue is already topical for existing cryptocurrencies, but is becoming even more policy relevant when state-backed digital currencies are introduced (Bech and Garratt, 2017).

For miners who forge the new blocks, i.e., solve the cryptographic puzzles related to adding new blocks into the blockchain, the main decisions are how much to invest in mining and how to carry out the mining if the blockchain has several forks. These decisions are affected by the incentives set in the design of blockchain protocols. An obvious incentive problem is how to reward the miners. Typical rewarding schemes include collecting transaction

fees and allocating them to those who win in the mining contest. In case of cryptocurrencies, it is also possible to reward the miners with seigniorage rents from the new units of the cryptocurrency, and this may affect the incentives for mining (Carlsten et al., 2016) as well as the price formation of the underlying asset (Pagnotta and Buraschi, 2018).

The second class of incentive problems relates to the security of the system and is also relevant in view of designing mechanisms for allocating rights to forge blocks. In economic terms, there are situations which involve a moral hazard problem; if the blockchain has two forks, a miner may have an incentive to forge blocks on both of them, which is not desirable because it leads to a situation where there is ambiguity on the contents of the ledger. As shown in this work this problem is in principle always present, even when there are several miners, but the incentives for the adverse behavior become smaller the more there are miners. Hence, letting more than one miner to forge blocks is an obvious way to alleviate the moral hazard problem.

Many of the decision problems related to the mining of new blocks have previously been addressed in game theoretic context with the emphasis on the game between the miners (Kroll et al., 2013; Eyal and Sirer, 2014; Sapirshtein et al., 2016; Houy, 2016; Dimitri, 2017; Biais et al., 2018). See Abadi and Brunnermeier (2018) and Sockin and Xiong (2018) on models of cryptocurrency markets involving consumers, miners, and developers. This paper considers the allocation of rights to forge blocks from a mechanism design point of view, and the equilibrium behavior of miners will be only briefly discussed. In particular, the capacities and costs of miners are not treated as choices but rather taken as exogenously given. The proof of work mechanism is not a unique example of using a contest in finding a solution for a given problem. Contests or tournaments have been frequently used in procurement, R&D, and labor markets as mechanisms for inducing innovation and mitigating moral hazard. In particular, auctioning the rights to participate in contests has been previously studied by Fullerton and McAfee (1999), and auctions will also be considered in this work.

In a decentralized environment where it is easy to preserve anonymity, it is desirable that there is no incentive for any participant of the mechanism to enrol several times with a different identity. This property is referred to as sybil proofness (Babaioff et al., 2012). In the literature on auctions, the related concept of false-name proofness has been discussed by Yokoo et al. (2004) and Ausubel and Milgrom (2005). The proof of work contest is shown to be unique among the randomization mechanisms that are sybil proof, symmetric, and do not involve messaging and payments. It is also the unique deterministic mechanism that treats the participants symmetrically and does not involve any messaging between the participants and the protocol.

The characterization of the PoW contest indicate that credible alternatives for it require allowing for messaging between the participants and the protocol, or payments such as participation fees. Two classes of alternatives are proposed in this work. The first is called proof of pay contests, where a predetermined number of participation rights are allocated at random such that the probabilities of getting them are proportional to the payments. These mechanisms are characterized by a set of elementary properties, of which most notable is sybil invariance: dividing a fixed sum between a miner and his sybil always leads to the same expected payoff. Second, single-run auctions are proposed as allocation mechanisms for rights to forge blocks. In these auctions the participants submit bids to the protocol which determines who will get the right to participate in the mining contest. However, it is shown that no single-run auction can treat the participants symmetrically and be sybil proof at the same time.

In Section 2, we describe the mining contest and the nothing at stake moral hazard problem arising from the forks of a blockchain. The proof of work contest is analyzed in Section 3 and the generalization of the proof of stake mechanism for allocating several mining rights is introduced in Section 4. Auctioning the rights to participate in the mining contest is studied in Section 5. Conclusions are discussed in Section 6.

2. Mining under Moral Hazard

The set of possible agents to carry out the addition of new blocks is denoted by $I = \{1, \dots, n\}$. In this work these block-generating agents are simply called miners. Each miner $i \in I$ has a hashing capacity k_i, which is often measured in terms of hash rate (number of computations per second). These capacities determine the probabilities of winning in the mining contest, where a set of miners compete for solving a given cryptographic puzzle. The one who presents a solution first wins the contest.

Let us describe the mining contest in more detail. Let x_i be the waiting time of a miner for solving the puzzle. The waiting time is an exponentially distributed random variable with parameter k_i/d, where d is a numerical indicator of the difficulty of the puzzle. Hence, the hashing capacity determines how fast a miner is expected to come up with a solution. The difficulty parameter is typically set by the protocol such that the expected time for finding new blocks is small enough. It follows that $\min\{x_i\}$, i.e., the time it takes for someone to solve the puzzle, is exponentially distributed with parameter $k_I = \sum_i k_i/d$. For a single miner $i \in I$ the probability of winning is then $p_i(k) = k_i/k_I$, where $k = (k_1, \dots, k_n)$. Note that it is assumed that no

participant of the mining contest exists before the puzzle is solved. Hence, the mining contest is simply a Tullock contest (Tullock, 1980).

The reward from winning the mining contest is set exogenously and is denoted by r. The costs of performing the task are $c_i \geq 0$, $i \in I$. Note that the cost is actually a random variable that depends on how long the capacity of a miner has to run. However, assuming that the difficulty d is chosen such that the expected time is fixed, the cost can be taken as the expected cost of running the capacity until the puzzle is solved by some of the miners.

The choice of the miners to perform the forging of new blocks can be regarded as a mechanism. A mechanism sets the rules for the participation in the contest of solving the puzzle, i.e., the mining contest. The first element of a mechanism is the message space M. A participant sends a message $m_i \in M$ to the mechanism, the profile of messages is denoted by $m = (m_1, \ldots, m_n)$. The second element consists of probabilities $p_i(m)$ of becoming selected when messages corresponding to profile m have been sent to the mechanism. The third element are the payments $f_i(m) \geq 0$ for each participant of the mechanism. To simplify matters it is assumed that all miners participate in the mechanism, i.e., participating in the mechanism gives higher expected profits than miners' reservation prices. There is also an obvious requirement for the mechanism; with probability one at least one miner can participate in the contest, because otherwise the cryptographic puzzle would remain unsolved.

Payments f_i ,$i \in I$, form an important element of the mechanism. In particular, there are several ways to impose participation fees. One is to require deposits of collateral from the participants—sometimes called stakes. Another is to require payment to the mechanism or payment to someone else. These are sometimes implemented even as wasting of money, so called proof of burn. One particular payment scheme would be to personalize the task and reward; miners could announce the difficulty level they want to solve and the reward is conditioned on that.

Ideally, if there would not be any security or incentive problems related to adding blocks, it would be socially optimal, in terms of minimizing costs, to let the mining be carried out by the miners with the smallest costs. In the extreme case there would be only one miner, which would make the blockchain vulnerable to an attack by that party. There is also a less severe moral hazard problem with one miner that arises when the blockchain has forked. Namely, in a case of a fork the miner can forge blocks on both branches and obtain the reward for sure. This is because it may happen that the other chain becomes the consensus chain in which case the miner looses the reward if he has not invested in it. It should be emphasized that the actual probability of loosing the reward in this case depends on the consensus mechanism.

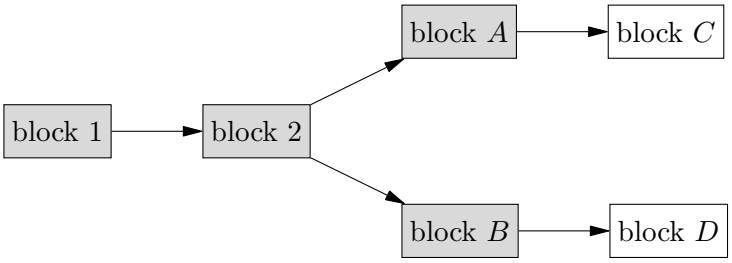

Figure 1: Schematic illustration of a blockchain fork.

The assumption that a miner can forge blocks on both (or more generally on any) branches of the chain means that the protocol itself cannot prevent this nor it is possible to make the reward contractible upon the added blocks. If it was possible to punish miners from adding several blocks, e.g., by requiring registration, it would become possible to prevent the moral hazard.[2] Throughout this work it is assumed that the reward can not be conditioned on anything else than having the mined block as a part of the consensus chain.

Let us next consider the moral hazard problem in the case of fork in more detail. First, the moral hazard problem related to blockchain fork is not only related to the case of having one miner but it is present more generally. For example, if there is one miner with significantly higher capacity than others, this single miner may find it optimal to mine both of the two branches of a forked blockchain. This general morel hazard is considered below.

A schematic example of a fork is presented if Figure 1, where A and B are two blocks that start separate subchains. Given that a miner has found a new block to one of the branches, let us say block C, he faces the problem of deciding whether to start mining the B-branch. If successful, he is the first to find the block D. Having found both blocks C and D would guarantee sure reward regardless of which of the branches becomes the consensus chain in the end. However, from the viewpoint of the users of the blockchain, maintaining the fork is not desirable. Moreover, usually miners cannot be punished from behaving in this manner. One simple reason is that miners can always use sybil identities when they publish blocks, which means that they can publish blocks C and D simultaneously by using two different identities. Punishing from undesirable behaviour is not possible unless there is a centrally managed registry of miners. Hence, in essence the miners have hidden actions as in

[2]Punishing miners from adverse behavior is part of the CASPER protocol designed for Ethereum blockchain.

the more conventional moral hazard setups.

Let p be the probability that the reward is lost in case of forging a block on only one of the branches. This probability is determined by the blockchain consensus protocol and ranges from zero to one half, and is taken as exogenously given in this work. The fork continues only when it happens that a miner first finds a solution to one of the forks and then solves the second puzzle. This requires that in the expectation when a miner has solved one puzzle he is better off when trying to solve the second one:

$$\mathbb{E}_{k_{-i}}\left[\frac{k_i}{k_i+\sum_{j\neq i}k_i}\right]r-c_i\geq(1-p)r.$$

Note that the right hand side of the above expression is the expected value of a miner given that he has already solved one puzzle. The left hand side is the expected value when having solved the puzzle in only one of the branches. In other words, a miner who has a high probability of solving the puzzle may be willing to continue the fork.

The lower bound of the cost of solving a puzzle is zero. For zero costs the above condition reduces to

$$\mathbb{E}_{k_{-i}}\left[\frac{k_i}{k_i+\sum_{j\neq i}k_i}\right]\geq(1-p).$$

This condition leads to a threshold for k_i such that it is optimal to mine both branches for capacities above the threshold, when the mining is costless. Let $\kappa(n)$ stand for this threshold. Below result states that the more there are miners the higher the threshold, i.e., the smaller the incentives to continue a fork. The proof is presented in the Appendix.

Proposition 1. *Assume that k_j are i.i.d. random variables that are drawn from a distribution that has a continuous cumulative distribution function on $[\bar{k},\infty)$, where $\bar{k}>0$. The function $\kappa(n)$ is increasing and unbounded.*

The above result has an important implication for the probability that there is moral hazard in the mining contest. Assume that the capacity distribution is non-atomic and has bounded support with an upper bound k_u. By the above result, there is a smallest number n such that $\kappa(n)\geq k_u$. Hence, the prior probability of a moral hazard is zero for large enough mining contests. This means that the PoW contest is likely to minimize the probability of moral hazard.

Note that when the fork involves more than two chains, the benefit from mining all of them becomes smaller than in the case of just two branches.

Hence, considering the case of fork with two branches is sufficient. Note also that the probability that a single miner is prone to moral hazard is always reduced by adding miners. Hence, having more miners is likely to decrease the risk of moral hazard and increase the safety of the blockchain. The safety is not only related to having miners that are prone to moral hazard but also the probability that such miners would be the ones to win the contest for solving the puzzle.

3. Characterizations of the Proof of Work Contest

In this section the purpose is to describe sets of requirements for a mechanism that are only satisfied by the PoW contest and hence make it uniquely different from all other mechanisms. Let us begin with one desirable property of the PoW contest: symmetric treatment of the participants. A mechanism is symmetric if miners sending same messages are treated the same way. A stronger form of equal treatment, anonymity, will be discussed later on.

Definition 1. The mechanism is symmetric if $m_i = m_j$ for $i \neq j$, $i, j \in I$ implies that $p_i(m) = p_j(m)$ and $f_i(m) = f_j(m)$.

The PoW contest can be regarded as a deterministic mechanism where each participant is accepted for sure. Hence, it is natural to begin with deterministic mechanisms; a mechanism is deterministic if $p_i(m) = 0$ or 1. When the participants are not allowed to send any messages and the mechanism satisfies the symmetry requirement, all the participants are accepted in the contest. Otherwise, there would not be anyone to solve the puzzle. Hence, we can make the following observation.

Proposition 2. *A deterministic mechanism with an empty message space is symmetric if and only if it is the PoW contest.*

When allowing the mechanism to be random or stochastic there are several alternatives that satisfy the symmetry assumption and do not require any messaging. For example, allocating the right to participate randomly to a single participant is a symmetric mechanism. However, the problem with this particular mechanism is that the probability of becoming selected is increased by participating multiple times. Because participating multiple times is undesirable, the mechanism should satisfy the property where such behavior does not increase anyone's expected payoff.

To suppress the notation, let us denote the type of miner i by $t_i = (k_i, c_i) \in T = [\bar{k}_i^1, \bar{k}_i^2] \times [\bar{c}_i^1, \bar{c}_i^2]$, and set

$$v(m, t_i|t_{-i}) = \mathbb{E}\left[\frac{rk_i}{k_i + \sum_{j\neq i} k_j} - c_i \Big| m\right].$$

As usual, subscript $-i$ refers to other miners than $i \in I$. Note that the mechanism determines the total capacity k_I in the mining contest, because the probabilities of becoming accepted in the contest depend on the messages. Hence, the expectation in the valuation of the contest is over $k_1, \ldots, k_n$ conditional on m. The miners' behavior in the mechanism can be conditioned on the type t_i. Hence, players' strategies are allowed to depend on t_i, $i \in I$. Let $\sigma_i : T \mapsto M$ stand for the strategy of miner $i \in I$. The expected value from sending message m_i is

$$\begin{aligned} &V(m_i, t_i|\sigma_{-i}) = \\ &\mathbb{E}_{t_{-i}}\left[p(m_i, \sigma_{-i}(t_{-i}))v((m_i, \sigma_{-i}(t_{-i})), t_i|t_{-i}) - f_i(m_i, \sigma_{-i}(t_{-i}))\right], \end{aligned}$$

Let (m_i^2, m_{-i}) denote the composition of m_i, m_{-i}, m_{n+1}, which is the set of messages submitted originally appended with message m_{n+1}, i.e., $m_i^2 \in M \times M$. In the following definition $p(m_i^2, m_{-i})$ denotes the probability that miner $i \in I$ gets accepted in the contest if he sends a messages $m_i \in M$ with his true identity and another message $m_{n+1} \in M$ with a false identity of another miner $n+1$, and the rest of the miners send messages listed in m_{-i}. It is assumed that each participant of the mechanism only observes his own message. Formally, the setup is a game of incomplete information where a miner has a belief over the other miners messages. The expected value of a miner with a sybil identity is

$$\begin{aligned} W(m_i^2, t_i|\sigma_{-i}) = \\ &\mathbb{E}_{t_{-i}}\left[p(m_i^2, \sigma_{-i}(t_{-i}))v((m_i^2, \sigma_{-i}(t_{-i})), t_i|t_{-i})\right. \\ &\left.-f_i(m_i^2, \sigma_{-i}(t_{-i})) - f_{n+1}(m_i^2, \sigma_{-i}(t_{-i}))\right]. \end{aligned}$$

Definition 2. The mechanism is sybil proof if there are no $i \in I$, σ_{-i}, and no pair of messages $m_i^2 = (m_i, m_{n+1}) \in M \times M$ such that

$$W(m_i^2, t_i|\sigma_{-i}) > \max_{m_i \in M} V(m_i, t_i|\sigma_{-i}).$$

As shown below the proof of work contest is characterized by symmetry and sybil proofness when there are no messaging and payments, i.e., $M = \emptyset$ and $f_i(m) = 0$ for all $i \in I$.

Proposition 3. *A mechanism with an empty message space and no payments is symmetric and sybil proof if and only if it is the PoW contest.*

Proof. When there are no payments, there is no cost of participating multiple times. Hence, sybil proofness implies that the probability of getting accepted is independent of the number of times the miner participates. Note

that participating multiple times is costless, the only thing that is affected by participating multiple times is the probability of getting accepted in the contest. Due to symmetry and having an empty message space, the probability of getting accepted cannot be conditioned on the identities of the participants but only on their number.

Let $p(i, n+1|n+1)$ be the probability of miner i or his sybil $n+1$ to be accepted given that there are n participants initially. By sybil proofness $p(i|n) = p(\{i, n+1\}|n+1)$, which implies that the probability of a set of miners to be accepted is independent of n. By the symmetry assumption $p(i|n) = p$. Hence, $p(\{i, n+1\}|n+1) = 2p(1-p) + p^2$ and $p(1-p) + p^2 = p$, which implies that either $p = 0$ or $p = 1$. The puzzle is not solved unless $p = 1$. □

The results presented in this section imply that the relevant alternatives for the PoW contest require either messaging between the miners and the protocol (in addition to sending the mined blocks) or payments, or both. Evidently, there are plenty of such mechanism, including the proof of stake and various auction formats. The proof of stake mechanism in which one of the miners gets the right to forge the next block can be embedded in a more general class of mechanism discussed in the next section.

4. Proof of Pay Contests with Multiple Mining Rights

Let us first observe that mechanisms where the probability of getting a permission to forge blocks genuinely depends on the message, should involve payments. To be more specific, when the probability of getting accepted into the mining contest increases when having a sybil sending a suitable message, the only way to obtain sybil proofness is to impose payments on sending messages.

Remark 1. If $p(m_i^2, m_i)$ is increasing for some choice of $m'_{n+1} \in M$, then the mechanism cannot be sybil proof unless $f_i(m) > 0$ all $i \in I$.

Having increasing probability to be accepted in the mining contest implies that without payments, all the participants would submit as many messages as possible. Hence, such a mechanism would not be feasible unless the number of participants (and or messages) was limited, or there are positive payments that prevent participants from submitting multiple messages under different identities.

One popular suggestion for a mechanism to choose one miner to carry out block addition is the proof of stake and its variants involving different ways to impose participation fees for the participants. The main idea in this

mechanism is that the participants need to invest in the mechanism in some form, and the probability of becoming selected to do the mining without any contestants is proportional to the size of the investment.[3] In principle, it does not matter how the investment is done; whether there is a deposit of collateral, wasted money, wasted time, or memory. What is important is that there is a cost to pay. For example, the requirement to deposit collateral causes costs to the participants; there is always an opportunity cost of capital. For the purposes of this work it is not essential how the costs are imposed, what is relevant is that participation is no longer free.

In the simplest case the right to forge a block is assigned randomly such that the probability of getting the right is proportional to the paid cost. Let $b_i \geq 0$ denote the bid or payment made by miner $i \in I$. The probability that miner i gets the right to mine a block is $p(b_i, b_{-i}) = b_i / \sum_j b_j$ in the usual proof of stake mechanism. Here the messages are simply the bids b_i, $i \in I$, and $f_i(b) = b_i$ for all $i \in I$. Hence, the question of allocating rights is turned into another Tullock contest. In principle, it is possible to define more general Tullock contests with probabilities of winning a right of the form $p(b_i, b_{-i}) = g(b_i)/(\sum_j g_j(b_j))$ for some non-negative function g, see Skaperdas (1996) on axiomatizations of contest success functions.

The proof of stake mechanism is symmetric and sybil proof when at least some of the miners has a positive bid; if a miner chooses a bid that maximizes the expected payoff from the mechanism, there is no reason to submit another bid because that would only lead to a smaller expected payoff. However, this mechanism is vulnerable to the moral hazard in the case of a fork. An obvious alleviation of the moral hazard problem is to allocate more than just one mining right. Indeed, the proof of stake with a single right to forge blocks can easily be generalized for allocating multiple rights to participate in the mining contest.

Assume that there are $N \geq 1$ participation rights into the mining contest. Each right is allocated to the participants according to their bids such that miner i receives each right with probability $p(b_i, b_{-i})$. Hence, the rights are allocated as if there was a separate proof of stake contest for each of the N rights. This mechanism is referred to as the N-PoP mechanism. It should be emphasized that in this work it is assumed that all the rights are allocated simultaneously, although in practice the allocation could be done sequentially conditioning on the information on who has obtained the previous rights.

[3] In some implementations of proof of stake, e.g. in BlackCoin, Cardano, Nxt, and Peercoin, the random selection of a miner is not conditioned only on stakes but also on other properties of the miners.

Note that there is a positive probability that one miner gets all the rights and does not face any competition in the mining contest. However, the probability of this to occur can be controlled by choosing the number of rights to be allocated large enough. For example, if one miner has 0.5 share of the bids, then the probability that this miner receives all the rights is about 3% for $N = 5$. Hence, the risk of moral hazard can be reduced considerably even when the number of rights to be allocated is relatively small.

The N-PoP mechanism is sybil proof when at least one bid is always positive.

Proposition 4. *The N-PoP mechanism is a sybil proof mechanism for any $N \geq 1$ when $\sum_j \sigma_j(t_j) > 0$ for all types t_j.*

Proof. Let σ_{-i} be any strategy profile for other players than i, and let b_i^* be an optimal bid for player i with capacity k_i. By the assumption, at least σ_{-i} one player always submits a positive bid. Hence, the probabilities of getting the rights are defined without ambiguity. Using a false identity and bidding b_{n+1} would lead to the expected payoff corresponding to bidding $b_i^* + b_{n+1}$ in the first place and paying $b_i^* + b_{n+1}$. However, by the optimality of b_i^* this cannot give higher expected payoff than b_i^*. Hence, the mechanism is sybil proof. □

It follows from the above result that when there is a positive minimum bid, the mechanism is sybil proof. Having a positive minimum bid implies that there will not be a type profile in which none of the miners would bid anything.

Corollary 1. *The N-PoP mechanism is sybil proof when there is a minimum bid $\bar{b} > 0$.*

The proof of pay mechanisms are not only sybil proof but they satisfy a related condition called sybil invariance. This condition says that the expected payoff of a miner does not change regardless of how he allocates any fixed amount between himself and his sybil.

Definition 3. The mechanism is sybil invariant when $M = \mathbb{R}_+$ and

$$V(m_i, t_i|\sigma_{-i}) = W(m_i^2, t_i|\sigma_{-i})$$

for all $m_i^2 = (m_i', m_{n+1})$ with $m_i', m_i, m_{n+1} \geq 0$ such that $m_i' + m_{n+1} = m_i$.

Note that sybil invariance does not imply sybil proofness. However, sybil invariance implies symmetry between a miner and his sybil.

Let us next consider the characterization of the N-PoP mechanism. First, the N-PoP mechanism belongs to a class of mechanisms in which the number of rights is binomially distributed: the probability that bidder i wins k rights out of N is binomially distributed with parameter $p_i(m)$. Having binomial distribution is reasonable, because it simply means that obtaining the rights can be considered independent trials. Hence, it is in essence a form of independence assumption.

The next assumption is that the expected payoff is zero if a miner does not bid anything when at least some of the other miners leave a positive bid. Evidently, this property holds for N-PoP mechanisms.

Definition 4. The mechanisms satisfies no award for null condition when $M = \mathbb{R}_+$ and if $m_j > 0$ at least for one $j \in I$, then the expected payoff for miner i is zero if $m_i = 0$.

We also need anonymity when characterizing the N-PoP mechanism. In the following π denotes the permutation of labels of miners, $\pi(i)$ is the label in the new permuted labeling and $\pi(m)$ is the vector of messages corresponding to the new labeling.

Definition 5. The mechanism is anonymous if $p_i(m) = p_{\pi(i)}(\pi(m))$ and $f_i(m) = f_{\pi(i)}(\pi(m))$.

Anonymity means that the labels of miners do not affect in the mechanism regardless of messages. Hence, neither symmetry nor sybil invariance implies anonymity.

Below it is shown that any mechanism that is sybil invariant with no award for null condition and binomial over N rights is the N-PoP mechanism. The proof of the result is presented in the Appendix.

Proposition 5. *Assume that $n \geq 3$, $M = \mathbb{R}_+$, and $m_i > 0$ for some $i \in I$, and $f_i(m) = m_i$ for all $i \in I$. An allocation mechanism for N rights is the N-PoP mechanism if and only if it is sybil invariant, the right is allocated to someone with probability one, the mechanism satisfies no award for null condition and anonymity, and the number of rights that each miner gets is binomially distributed with N trials.*

For the usual proof of stake, i.e., the 1-PoP mechanism, the assumption on binomial distribution over the rights is void.

Corollary 2. *Assume that $n \geq 3$, $M = \mathbb{R}_+$, and $m_i > 0$ for some $i \in I$, and $f_i(m) = m_i$ for all $i \in I$. An allocation mechanism for a single right is the proof of stake mechanism if and only if it is sybil invariant, the right is allocated to someone with probability one, and the mechanism satisfies no award for null condition and anonymity.*

Finally, let us turn to the question on the existence of Bayesian Nash equilibrium in the N-PoP mechanism. In equilibrium the bidding strategy depends on the valuations of other miners, i.e., their distribution. To formalize the analyses, it is assumed that either costs or capacities are common knowledge. Hence, the bidding strategies depend on capacities or costs. The existence of Bayesian Nash equilibrium can be shown when the bids are limited to a compact interval on positive real axes. The proofs of the following results are presented in the Appendix and they rely on the existence of Bayesian Nash equilibrium under the single crossing property Athey (2001), see also Wasser (2013) on an application of single crossing in contests with incomplete information. It is assumed that nobody who participates in a mining contest exists the contest before the puzzle is solved. If exiting was allowed the setup would resemble a war of attrition with incomplete information (Bulow and Klemperer, 1999).

Proposition 6. *Assume that the common prior over capacities is bounded and atomless and that the players' available bids are on interval* $[\bar{b}^1, \bar{b}^2]$*, where* $\bar{b}^2 \geq \bar{b}^1 > 0$*. The N-PoP mechanism has a Bayesian Nash equilibrium where the players' bidding strategies are non-decreasing functions of their capacities.*

In practice, the capacity shares may become revealed over time when the shares of wins in past mining contests are publicly known. Hence, it is also important to consider the case of uncertainty over the cost. For this case we have an analogous existence result.

Proposition 7. *Assume that the common prior over costs is bounded and atomless and that the players available bids are on interval* $[\bar{b}^1, \bar{b}^2]$*, where* $\bar{b}^2 \geq \bar{b}^1 > 0$*. The N-PoP mechanism has a Bayesian Nash equilibrium where the players' bidding strategies are non-decreasing functions of their costs.*

As an example, consider the case of n miners with the same capacities and costs, in which case the value of the contest $v = k_i / \sum_j k_j = 1/n$, and the payoffs are $p_i(b)v - b_i$. Assuming $p_i(b) = b_i / \sum_j b_j$, the first order conditions yields

$$\frac{v \sum_{j \neq i} b_j}{\left(\sum_j b_j \right)^2} = 1,$$

which gives $b_i = vn^2/(n+1)^2$ when assuming symmetric bids; $b_i = b_j$ for all $i, j \in I$. Hence, the bid is below the valuation v, which shows that the N-PoP mechanism is not truthful in the sense that in equilibrium bidders would bid according to their true valuations. Note, however, that in the limit when n goes to infinity the equilibrium bids approach to the value of the contest.

5. Auctioning the Rights to Forge Blocks

One alternative to choose the miners who are allowed to forge blocks is to auction the rights to participate in the mining contest. In general, in any single-round auction mechanism the rights are allocated according to simultaneously placed sealed bids by the participants. Because there are multiple rights that are sold, a bid can be regarded as a vector of prices that a participant is willing to pay for each additional right. In the following a bid is denoted by $b^i = (p_i^1, \ldots, p_i^{S_i})$, $i \in I$, where $p_i^j > 0$ is the price that the bidder is willing to pay for j'th right to participate in the mining contest. Here $S_i \leq N$ is the largest number of rights that the bidder is willing to buy, i.e., for the $S_i + 1$'th right the willingness to pay is zero. The set of allowed bids is denoted by B, i.e., B is composed of all vectors of length N or less with positive components.

In the auction mechanism the message space consists of the bid vectors and the mechanism determines how many rights each bidder receives and the price paid by each participant. Technically, an auction mechanism determines which bids are winning by maximizing the sum of accepted bids under the constraint that each unit can be allocated to at most one bidder. An important element of an auction mechanism is the tie-breaking rule; how the rights are allocated when there are several solutions for the winner determination problem, i.e., multiple solutions to the maximization of total sum of bids given the number of rights to be allocated.

In many cases multiunit auctions have decreasing differences; the marginal gain from an additional unit is decreasing in the number of units. In this respect, allocating rights to participate in the mining contest is different; the valuation of an extra right is increasing in the number of rights that the miner has. To show this, let us denote the value of the contest with S participants by

$$v(t_i, S) = \mathbb{E}_{k_{-i}} \left[\frac{k_i}{k_i + \sum_{j \neq i} k_j} \middle| S \right] r - c_i.$$

The more there are competitors in the contest, the less valuable an extra participation right is for a miner, or to put it other way; the more a miner possesses mining rights, the more valuable an additional right is.

Proposition 8. *The differences $v(t_i, S+1) - v(t_i, S)$, $i \in I$, are decreasing in S.*

Proof. Without the loss of generality we may consider the case when $i = 1$.

Let us set

$$\Delta(S) = v(t_1, S+1) - v(t_1, S) = rk_1\mathbb{E}\left[\frac{1}{k_1 + \sum_{j=2}^{S} k_j} - \frac{1}{k_1 + \sum_{j=2}^{S-1} k_j}\right]$$

The difference is negative;

$$\Delta(S+1) - \Delta(N) = rk_1\mathbb{E}\left[\frac{-\left(\sum_{j=1}^{S-1} k_j\right)\left(\sum_{j=2}^{S+2} k_j\right)}{(k_1 + \sum_{j=2}^{S+1} k_j)(k_1 + \sum_{j=2}^{S} k_j)(k_1 + \sum_{j=2}^{S-1} k_j)}\right].$$

□

The above result means that having more rights is always beneficial, and the marginal gain from an extra mining right is increasing. When there is no budget constraint this implies that a bidder who is willing to bid for two rights is willing to bid for all of them.

Corollary 3. *If a bidder is willing to buy* 2 *rights, then he is willing to buy all of them.*

Let us next consider in more detail the case of ties. The possibility that an auction ends up with two or more bidders having the same bid is an important reason for submitting multiple small bids, which is a particular case of a failure of sybil proofness. When the mechanism satisfies the symmetry assumption the tie breaking rule should satisfy it too. An example of a symmetric tie breaking rule, is a lottery where the rights for which there is excess demand are allocated randomly to the bidders whore are willing to buy them such that the probabilities of obtaining them are the same.

Definition 6. A tie-breaking rule is symmetric if all the bidders with the same bids have the same expected number of rights in the case of a tie.

Let us now formulate the result on the impossibility of sybil proofness. The result is not only related to auctioning mining rights but it is a more general property of multi-unit auctions.

Proposition 9. *There is no sybil proof symmetric single-round auction mechanism with bids B where loosing bids need not pay. Sybil proofness is attained for such auctions only when the tie-breaking rule is asymmetric.*

Proof. Symmetry implies that bidders with exactly the same bids are treated symmetrically. Now assume that there are two symmetric bidders whose bid all the rights with price 1. Moreover, assume that the valuations are common

knowledge. Since the mechanism is symmetric both bidders have the same expected number of rights, i.e., $N/2$ for both of them. In this case, there is an incentive to have a sybil that bids identically with the bidder, because this would increase the expected value of rights to $2N/3$. Note also that loosing bidders, i.e., those who do not get a right do not need to pay. Hence, no symmetric single-round auction is sybil proof. Moreover, a necessary condition for sybil proofness is that the tie-breaking rule treats the bidders asymmetrically

□

It follows from Proposition 9 that a single-round auction mechanism can be sybil proof only when the tie breaking rule treats the participants asymmetrically. It should be noticed sybil-proofness can be attained in the domain of allocation problems without ties (Iwasaki et al., 2005; Yokoo et al., 2001).

There are several ways to define asymmetric tie-braking rules. One possibility is to use a seniority rule; in the case of a tie more senior bidder wins. Seniority can be defined for instance in terms of previous participation in the mining contest. Another way to obtain sybil proofness would be to let the participants to make multiple bids in the first place. In particular this could be done together with payments, which is discussed below.

A single-round auction mechanism is an all pay auction when each bidder pays at least $\min_j p_i^j$ for each bid even when not getting any rights. When submitting bids is costly the auction becomes sybil proof. This is because the marginal benefit from an extra bid is non-increasing. Hence, there is a finite upper bound for the optimal number of bids.

Remark 2. Any all pay auction where each bidder pays at least $\bar{p} > 0$ for each bid is sybil proof, when each bidder is allowed to submit sufficiently many bids.

The lack of sybil proofness means that auctions are not necessarily practical for allocating rights to participate in the mining contest unless the participation in the mechanism can be controlled, which is possible in permissioned ledgers with a single private party who can run the auction. Moreover, in such a centralized case the concern on sybil proofness is less severe. For instance, the auctioneer may restrict the participation into the auction to previously known reputable miners. The benefit of auctions is that they may have notable efficiency gains over the PoW and the N-PoP mechanism. An obvious source of such gains is the smaller amount of wasted effort when the mining is carried out by the most efficient miners. In practice, the auction could be run in a day-ahead fashion as in the case of retail electricity markets, which would lead to a situation where the mining is carried out by different

miners at different hours depending on where they are located and where the price of electricity is the lowest.

6. Conclusions

The question of allocating rights to forge blocks has received surprisingly little attention among the developers of various blockchain technologies, although it is widely admitted that the commonly used proof of work mining contest requires large amounts of wasted energy. The most notable alternative that has been suggested for the proof of work is the proof of stake mechanism where only one miner at a time forges a block, and the probabilities of getting selected are proportional to the miners' stakes or payments. This paper is the first to study the allocation of mining rights systematically starting from the desiderata of allocation mechanisms.

Despite of its apparent inefficiency, the proof of work mining contest has several attractive features. First, it is sybil proof, which means that there is no reason for any miner to use multiple false identities when participating into the mining contest. Second, it is symmetric, i.e., it treats similar participants the same way. Moreover, any other mechanism for allocating rights to forge new blocks that would satisfy these properties should allow for payments and messaging between the participants of the mechanism and the protocol that assigns the rights to forge blocks.

One feature in the mining contest is that a miner may have an incentive to maintain a fork of the blockchain, which is highly undesirable. In this work, this problem is viewed as a particular case of moral hazard due to incomplete information on the actual actions of miners. The moral hazard problem is exacerbated by the asymmetry of miners' capacities, especially, when there are only a few participants in the mining contest. Hence, the proof of work mechanism, in which there is free participation in the mining contest, is likely to reduce the moral hazard.

This work generalizes the proof of stake mechanism for multiple mining rights such that the resulting mechanism is sybil proof and symmetric. In essence the question is on a simultaneous use of the proof of stake mechanism for allocating a predetermined number of rights randomly to the participants with probabilities that are proportional to their payments. It should be emphasized that allocating more than just one right is a way to mitigate the moral hazard problem related to the mining of blocks when there is a fork in the blockchain.

When allocating multiple rights to participate in the mining contest, auctioning the rights is one possible alternative. This work is the first to propose auctions for this purpose in the context of blockchains. Auctions may have

significant efficiency gains compared to the proof of work and the proof of stake type of mechanisms. However, when ties are possible no single-round auction can be made sybil proof without violating the symmetric treatment of participants.

Appendix A. Auxiliary proofs

Appendix A.1. Proof of Proposition 1

The choice of n induces a measure over the total capacity k_{-i} of other miners than i. Let the cumulative distribution function μ_n correspond to this measure. The distributions satisfy $\mu_n(x) < \mu_{n+1}(x)$ for $x > \bar{k}$, because having more miners taken randomly from the same distribution necessarily increases the capacity. In essence, μ_{n+1} has the first order stochastic dominance over μ_n;

The function $f(x) = k_i/(k_i + x)$ is decreasing in x and goes to zero as x goes to infinity. The dominance relation implies

$$\int_0^\infty f(x)d\mu_n(x) < \int_0^\infty f(x)d\mu_{n+1}(x) \tag{A.1}$$

for any decreasing function f that is right continuous that goes to zero when x goes to infinity. To show that this is the case observe that by partial integration

$$\int_0^\infty f(x)d\mu_{n+1}(x) = f(x)\mu_{n+1}(x)\Big|_0^\infty - \int_0^\infty \mu_{n+1}(x)df(x).$$

Assuming that $f(x) \to 0$ when $x \to \infty$, we get

$$\int_0^\infty f(x)d\mu_{n+1}(x) = -\int_0^\infty \mu_{n+1}(x)df(x)$$

and likewise

$$\int_0^\infty f(x)d\mu_n(x) = -\int_0^\infty \mu_n(x)df(x).$$

Because f is decreasing, the inequality $\mu_n(x) < \mu_{n+1}(x)$ for $x > \bar{k}$ implies that

$$\int_0^\infty \mu_{n+1}(x)df(x) < \int_0^\infty \mu_n(x)df(x).$$

Hence, (A.1) holds.

At the threshold $\kappa(n)$ we have

$$\int_0^\infty \frac{\kappa(n)}{\kappa(n)+x} d\mu_n(x) = (1-p).$$

When n is increased

$$\int_0^\infty \frac{\kappa(n)}{\kappa(n)+x} d\mu_{n+1}(x) > (1-p)$$

by (A.1). Hence, the threshold is increasing as a function of n. The threshold is unbounded because the expected value of $\sum_{j\neq i} k_j$ goes to infinity when n goes to infinity. Namely,

$$\int_0^\infty \frac{\kappa(n)}{\kappa(n)+x} d\mu_n(x) \leq \frac{\kappa(n)}{\kappa(n)+(n-1)\bar{k}}.$$

Because the right hand side expression goes to zero as n increases, $\kappa(n)$ goes to infinity. This concludes the proof. □

Appendix A.2. Proof of Proposition 6

For the proof of Proposition 6, let us denote the expected value of a miner by

$$U_i(b_i, k_i; \sigma_{-i}) = \\ \mathbb{E}_{k_{-i}} \left[\sum_{j=1}^{N} p^j(b_i, \sigma_{-i}(k_{-i})) \mathbb{E}_{k_{-i}} \left(\frac{r k_i}{k_i + \sum_{j\neq i} k_j} - c_i \,|N-j \right) \right] - b_i.$$

According to the main result of Athey (2001) there is a monotone equilibrium in a game with incomplete information when the payoff functions satisfy the single crossing condition and the prior distribution over types is non-atomic. It is elementary to observe that the single crossing holds when the type is c_i, in which case the miners' payoff functions are simply linear in their types. Below lemma shows the single crossing condition when the type is the capacity.

Lemma 1. *Functions $U_i(b_i, k_i; \sigma_{-i})$, $i \in I$, satisfy the single crossing condition:*

$$U_i(b_i^L, k_i^H; \sigma_{-i}) - U_i(b_i^L, k_i^L; \sigma_{-i}) \geq 0$$

implies

$$U_i(b_i^H, k_i^H; \sigma_{-i}) - U(b_i^H, k_i^L; \sigma_{-i}) \geq 0$$

for all $b_i^H \geq b_i^L$, $k_i^H \geq k_i^L$ and σ_{-i}.

Proof. Consider the function

$$I(b_i, b_{-i}, k_{-i}, k_i) = \sum_{j=1}^{N} p^j(b_i, b_{-i}) \mathbb{E}_{k_{-i}} \left(\frac{rk_i}{k_i + \sum_{j \neq i} k_j} - c_i | N - j \right) - b_i$$

for a given vector b_{-i} of bids by other miners than i. The function $p^j(b_i, b_{-i})$ is increasing in b_i, and $(rk_i)/(k_i + k_{-i})$ is increasing in k_i. It follows that

$$\begin{aligned}
0 \leq & I(b_i^L, b_{-i}, k_{-i}, k_i^H) - I(b_i^L, b_{-i}, k_{-i}, k_i^L) = \\
& \sum_{j=1}^{N} p^j(b_i^L, b_{-i}) \left[\mathbb{E}_{k_{-i}} \left(\frac{rk_i^H}{k_i^H + \sum_{j \neq i} k_j} - c_i | N - j \right) \right. \\
& \left. - \mathbb{E}_{k_{-i}} \left(\frac{rk_i^H}{k_i^H + \sum_{j \neq i} k_j} - c_i | N - j \right) \right] \leq \\
& \sum_{j=1}^{N} p^j(b_i^H, b_{-i}) \left[\mathbb{E}_{k_{-i}} \left(\frac{rk_i^H}{k_i^H + \sum_{j \neq i} k_j} - c_i | N - j \right) \right. \\
& \left. - \mathbb{E}_{k_{-i}} \left(\frac{rk_i^H}{k_i^H + \sum_{j \neq i} k_j} - c_i | N - j \right) \right] \\
= & I(b_i^H, b_{-i}, k_{-i}, k_i^H) - I(b_i^H, b_{-i}, k_{-i}, k_i^L),
\end{aligned}$$

which in turn gives

$$U_i(b_i^H, k_i^H; \sigma_{-i}) - U_i(b_i^H, k_i^L; \sigma_{-i}) \geq U_i(b_i^L, k_i^H; \sigma_{-i}) - U_i(b_i^L, k_i^L; \sigma_{-i}) \geq 0.$$

Hence, the single crossing condition holds for all σ_{-i}. □

Appendix A.3. Proof of Proposition 5

It is elementary to observe that the N-PoP mechanism satisfies all the properties listed in the proposition. Hence, it is sufficient to show that any mechanism that satisfies the assumptions is the N-PoP mechanism.

Assume that the miners are symmetric in their types, i.e., $t_i = t$ for all $i \in I$ and there is no uncertainty, which means that the types are common knowledge. Note also that the strategies are common knowledge which means that the messages m_i are also common knowledge. Together with linearity of f this implies that

$$V(m_i, t_i | \sigma_{-i}) = G(p_i(m), v(1), \ldots, v(N)) - m_i,$$

where $v(k)$, $k = 1, \ldots, N$, are the values of the contest when miner i wins k out of N mining rights and $G(p_i(m), v(1), \ldots, v(N))$ is the expected value

over the binomial distribution with N trials and probability $p_i(m)$ for a success;

$$G(p_i(m), v(1), \ldots, v(N)) = \sum_{j=1}^{N} \binom{N}{j} p_i^j(m) \left(1 - p_i(m)\right)^{N-j} v(j).$$

Note that assuming that there is no uncertainty means that the expected payoff in the contest only depends on the number of mining rights and no longer on messages sent by other miners. To suppress the notation we drop the arguments $v(1), \ldots, v(N)$ from G in the following. Recall that $v(1), \ldots, v(N)$ are the same for each miner when assuming symmetric types.

Due to anonymity and symmetric types, any pair $i, j \in I$ can be regarded as a miner and his sybil. Anonymity guarantees that the label of the miner does not matter, only the message. Due to sybil invariance the payoff to the pair (i, j) satisfies

$$W(m_i^2, t_i | \sigma_{-i}) = W(s_i^2, t_i | \sigma_{-i}),$$

where $m_i^2 = (m_i, m_j)$, $s_i^2 = (s_i, s_j)$, and $m_i + m_j = s_i + s_j$. Let m denote the message profile with m_i^2 for i and j, and let s stand for the message profile with s_i and s_j for miners i and j while other miners send messages m_{-i}. Note that

$$W(m_i^2, t_i | \sigma_{-i}) = G(p_i(m) + p_j(m)) - m_i - m_j.$$

Hence, we have

$$G(p_i(m) + p_j(m)) = G(p_i(s) + p_j(s)),$$

which does not hold unless $p_i(m) + p_j(m) = p_i(s) + p_j(s)$. Note that the expected value over the binomial is different for different values of probabilities $p_i(m)$. This is means that $p_i(m)$ as a sharing rule of probability mass, satisfies pairwise reallocation proofness.

As a sharing rule of probability mass p_i has some important features in addition to pairwise reallocation proofness; $p_i(m) \geq 0$, $\sum_i p_i(m) = 1$ (at least someone gets a right), and $p_i(0) = 0$ when $m_j > 0$ for some $j \neq i$, which is implied by the no award for null condition for the mechanism.

The latter properties of p_i can be translated as non-negativity, efficiency, and no award for null for the sharing rule p_i. By Theorem 4 of Ju et al. (2007) the sharing rule $p_i(m_i)$ for the probability mass having these properties is the proportional rule $p_i(m) = m_i / \sum_j m_j$ when $n \geq 3$ and $m_i > 0$ for some $i \in I$. Hence, the ex ante probabilities are exactly the same as in the N-PoP mechanism. □

Acknowledgements

I thank Topi Miettinen, Peter Hans Matthews, and the seminar participants in the XL Annual Meeting of the Finnish Economic Association for their comments.

References

Abadi, J., Brunnermeier, M., 2018. Blockchain economics. Working paper.

Athey, S., 2001. Single crossing properties and the existence of pure strategy equilibria in games of incomplete information. Econometrica 69 (4), 861–889.

Ausubel, L., Milgrom, P., 2005. The lovely but lonely Vickrey auction. In: P. Cramton, R. S., Shoham, Y. (Eds.), Combinatorial Auctions. MIT Press.

Babaioff, M., Dobzinski, S., Oren, S., Zohar, A., 2012. On Bitcoin and red balloons. In: Proceedings of the 13th ACM conference on electronic commerce. ACM, pp. 56–73.

Bech, M., Garratt, R., 2017. Central bank cryptocurrencies. BIS Quarterly Review (September), 55–60.

Biais, B., Bisière, C., Bouvard, M., Casamatta, C., 2018. The blockchain folk theorem. Working paper.

Böhme, R., Christin, N., Edelman, B., Moore, T., 2015. Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives 29, 213–238.

Bulow, J., Klemperer, P., 1999. The generalized war of attrition. American Economic Review 89 (1), 175–189.

Carlsten, M., Kalodner, H., Weinberg, S. M., 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. ACM, pp. 154–167.

Cheah, E. T., Fry, J., 2015. Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. Economics Letters 130, 32–36.

Ciain, P., Rajcaniova, M., Kancs, A., 2016. The economics of BitCoin price formation. Applied Economics 48 (19), 1799–1815.

Dimitri, N., 2017. Bitcoin mining as a contest. Ledger 2, 31–37.

Eyal, I., Sirer, E. G., 2014. Majority is not enough: Bitcoin mining is vulnerable. In: International Conference on Financial Cryptography and Data Security. Springer, pp. 436–554.

Fullerton, R. L., McAfee, R. P., 1999. Auctioning entry into tournaments. The Journal of Political Economy 107 (3), 573–605.

Houy, N., 2016. The Bitcoin mining game. Ledger 1, 53–68.

Iansati, M., Lakhami, K. R., 2017. The truth about blockchain. Harvard Business Review 95 (1), 118–127.

Iwasaki, A., Yokoo, M., Terada, K., 2005. A robust open ascending-price multi-unit auction protocol against false-name bids. Decision Support Systems 39, 23–39.

Ju, B.-G., Miyagawa, E., Sakai, T., 2007. Non-manipulable division rules in claim problems and generalizations. Journal of Economic Theory 132, 1–26.

Kroll, J. A., Davey, I. C., Felten, E. W., 2013. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In: Proceedings of WEIS.

Li, X., Wang, C. A., 2017. The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. Decision Support Systems 95, 49–60.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. No publisher, available at https://bitcoin.com/bitcoin.pdf.

O'Dwyer, K. J., Malone, D., 2014. Bitcoin mining and its energy footprint. In: SSC 2014/CIICT.

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

Polasik, M., Piotrowska, A., Wisniewski, T. P., Kotkowski, R., Lightfoot, G., 2015. Price fluctuations and the use of Bitcoin: An empirical inquiry. International Journal of Electronic Commerce 20 (1), 9–49.

Saleh, F., 2017. Blockchain without waste: Proof-of-stake. Working paper.

Sapirshtein, A., Sompolinsky, Y., Zohar, A., 2016. Optimal selfish mining strategies in Bitcoin. In: International Conference on Financial Cryptography and Data Security. pp. 515–532.

Skaperdas, S., 1996. Contest success functions. Economic Theory 7, 283–290.

Sockin, M., Xiong, W., 2018. A model of cryptocurrencies. Working paper.

Tullock, G., 1980. Efficient rent seeking. In: J. Buchanan, R. T., Tullock, G. (Eds.), Toward a theory of the rent-seeking society. A & M University Press, Texas.

Wasser, C., 2013. A note on Bayesian Nash equilibria in imperfectly discriminating contests. Mathematical Social Sciences 66 (2), 180–182.

Yokoo, M., Sakurai, Y., Matsubara, S., 2001. Robust combinatorial auction protocol against false-name bids. Artificial Intelligence 130 (2), 167–181.

Yokoo, M., Sakurai, Y., Matsubara, S., 2004. The effect of false-name bids in combinatorial auctions: New fraud in internet auctions. Games and Economic Behavior 46 (1), 174–188.