frontiers
in Blockchain

ORIGINAL RESEARCH
published: 21 April 2020
doi: 10.3389/fbloc.2020.00016

Cryptocurrencies: Miner Heterogeneity, Botnets, and Proof-of-Work Efficiency

*Fabian Schär**

Faculty of Business and Economics, Center for Innovative Finance, University of Basel, Basel, Switzerland

Proof-of-work cryptocurrencies are heavily criticized for the alleged inefficiency of their mining mechanism. However, critics fail to distinguish between the resources that are used to secure the blockchain and those that are wasted. In this paper, we introduce a simple mining model and use this model to analyze the consensus protocol's efficiency, while accounting for the heterogeneity of the miners involved. We categorize the resources allocated by the miners as either useful or wasteful, and then use this to introduce a new measure of efficiency. We then demonstrate how this value depends on a set of potential miners and the variation of their marginal costs. Using this model, we then consider the existence of botnets and show how one could affect the security of the network. This analysis indicates that botnets can significantly change the mining landscape and, under certain circumstances, may lead to a dissipation ratio >1.

Keywords: bitcoin, blockchain, botnet, cryptocurrencies, mining, proof-of-work

OPEN ACCESS

Edited by:
Joerg Osterrieder,
Zurich University of Applied Sciences,
Switzerland

Reviewed by:
Gina C. Pieters,
University of Chicago, United States
Nicolas T. Courtois,
University College London,
United Kingdom

***Correspondence:**
Fabian Schär
f.schaer@unibas.ch

Specialty section:
This article was submitted to
Financial Blockchain,
a section of the journal
Frontiers in Blockchain

***Received:** 02 July 2019*
***Accepted:** 20 March 2020*
***Published:** 21 April 2020*

Citation:
Schär F (2020) Cryptocurrencies:
Miner Heterogeneity, Botnets, and
Proof-of-Work Efficiency.
Front. Blockchain 3:16.
doi: 10.3389/fbloc.2020.00016

1. INTRODUCTION

Bitcoin (Nakamoto, 2008) and similar cryptocurrencies employ a consensus mechanism referred to as proof-of-work. Participants allocate computational resources in an attempt to find a set of transactions and additional data, that satisfy a pre-defined set of conditions (i.e., a valid block). In the long run, the probability of success is a function of a participant's computing power in relation to the computing power of the other participants. The greater the relative contribution of an individual, the greater the probability that this individual will find the next valid block and claim the block reward.

From a game theoretical perspective, this mechanism can be simplified and modeled as a non-standard, all-pay auction with full information (Dimitri, 2017). Participants allocate resources to compete for an exogenously given reward (Sams, 2014), trying to maximize their expected return. In the absence of any barriers to entry, participants will allocate resources up to the value of the reward.

The increasing amount of computational resources used in this process and the fact that resource allocation has no effect on the number of transactions that can be processed by the network, has led to strong concerns about the efficiency of the proof-of-work consensus protocol (O'Dwyer and Malone, 2014). Proponents argue that the situation is not as straightforward as resources are used to secure the network. As more computing power is allocated, the blockchain becomes more secure, and it becomes harder to attack the chain and reverse transactions. A fair comparison to the existing payment systems would require the inclusion of any security measures employed by those systems as well as the risk of misconduct and rent-seeking by a monopolist (Berentsen and Schär, 2017, 2018). While we will not try to propose a solution to the efficiency debate in absolute terms, we strongly believe that a theoretical framework is needed to provide a better understanding of how the computing power is being used.

In this context, here we will introduce a model based on rent-seeking literature, in particular Tullock (1980), that allows us to classify the allocated resources as either useful or wasteful. The useful resources contribute to the security of the network, while the wasted resources have no social benefit to the system. This distinction allows for an analysis of the efficiency of the network while taking into account the effect of miners with differing marginal costs on the system. Depending on which miner contributes to the computing power, the security level and its cost to reach it may vary significantly.

We will first present the base model and discuss the case of $\bar{N} \geq 2$ homogeneous miners. We use this model to define the terminology and introduce our measure of network security. We will then relax the assumptions by allowing miners to be heterogeneous and show the effect that heterogeneity has on the dissipation ratio and network security. Next, we will introduce our efficiency measure, which combines dissipation and network security considerations. It represents the proportion of expenditures that directly serve to protect the network. Finally, we will consider the existence of botnets. We use the term botnet somewhat liberally in that we use it for any mining resources whose costs are not borne by their respective decision-makers, i.e., mining malware. We show how the presence of such resources may change the mining landscape and demonstrate how they affect the aggregate expenditures, security, and efficiency of the network.

2. MODEL

Let N be a set of $\bar{N} \geq 2$ potential miners denoted by n_i with $i \in \{1, \ldots, \bar{N}\}$. Each miner decides to use a certain hashing power[1] $h_i \geq 0$ to maximize its own expected payoff function, given by Equation (1). The hash rate allocation vector, $\boldsymbol{h}$, is of length $\bar{N}$ and includes all the individual hash rates, h_i, for each miner, n_i. The cost function, $c_i(h_i)$, is assumed to increase linearly in hashing power, h_i, such that $\frac{\partial c_i(h_i)}{\partial h_i} = \alpha_i > 0$ and $\frac{\partial c_i(h_i)}{\partial h_i^2} = 0$.

Miners compete for a reward. The value of this reward is exogenously given, and mining resources are in fact a function of the reward rather than *vice versa*. We represent the individual valuation of this reward by v_i and restrict $v_i = v > 0, \forall i$, where v represents the coinbase and the expected transaction fees. In contrast to the analogy of gold mining, this reward is, in the long run, independent of the respective choices for $\boldsymbol{h}$. The hashing vector only influences the allocation probabilities of this reward. Thus, cryptocurrency mining essentially corresponds to a rent-seeking game, where the prize corresponds to the block reward, v, and the probability, $p_i(\boldsymbol{h})$, is given by Equation (2).

$$\pi_i^e(\boldsymbol{h}, v_i) := \begin{cases} 0 & \text{if } \boldsymbol{h} = \boldsymbol{0} \\ p_i(\boldsymbol{h}) v_i - c_i(h_i) & \text{otherwise.} \end{cases} \tag{1}$$

$$p_i(\boldsymbol{h}) := \frac{h_i}{\sum\limits_{j \in N} h_j} \tag{2}$$

This setup describes a non-standard, all-pay auction, in which any miner i with $h_i > 0$ has a proportionate chance of winning the reward. Consequently, the miner's decision problem can be formalized as shown in Equation (3).

$$h^* = \underset{h_i \geq 0}{\arg\max}\ \pi_i^e(\boldsymbol{h}, v) \tag{3}$$

2.1. Homogeneous Miners

For now, we will only consider the case of homogeneous miners. Hence, $c_i(h_i) = \alpha h_i, \forall i = \{1, \ldots, \bar{N}\}$. Making use of homogeneity, the first order condition yields the profit maximizing h^* as shown in Equation (4), where $h_i = h^*, \forall i \in N$ corresponds to the symmetric Nash equilibrium.

$$h_i^* = \frac{(\bar{N} - 1)v}{\bar{N}^2 \alpha} \tag{4}$$

Figure 1 shows the optimal aggregated choices of h^* as a function of the number of potential miners $\bar{N}$ and the marginal cost/reward ratio $\frac{\alpha}{v}$. It becomes apparent that the aggregate hash rate increases in $\bar{N}$ and decreases in $\frac{\alpha}{v}$.

Plugging (4) back into (1) we get Equations (5) and (6), which can be interpreted as the individual and social profit functions, respectively.

$$\pi_i^e = \frac{v}{\bar{N}^2} \tag{5}$$

$$\sum_{i=1}^{\bar{N}} \pi_i^e = \frac{v}{\bar{N}} \tag{6}$$

As a consequence of an increase in aggregate hash rate expenditures, individual and social profits decrease with $\bar{N}$. Note, that in the homogeneous case, profits are unaffected by any

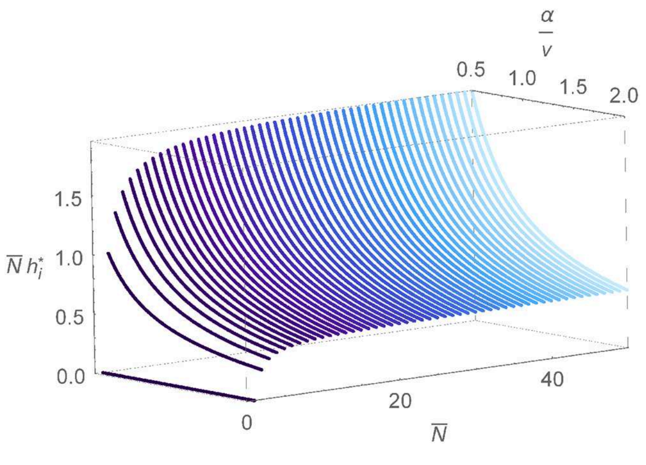

FIGURE 1 | Aggregate hash rate $h^*(\alpha, v)$ for each $\bar{N} = \{1, \ldots, 50\}$.

[1] i.e., a certain number of hashes per second.

changes in marginal costs α. An increase in α leads c.p. to a larger marginal cost/reward ratio $\frac{\alpha}{v}$. As shown in **Figure 1**, this causes a decrease in the total hash rate. At first, the drop could be falsely interpreted as a decrease in network security. However, assuming that a potential attacker is subject to the same terms as anyone else, α has no effect on the security of the network. This is shown in the proof of Proposition 2.

In rent-seeking literature, it is common to express social costs in relative terms to the value of the reward. This ratio as defined in Equation (7), is usually referred to as the dissipation ratio. Plugging Equation (4) into (7) and making use of homogeneity, we obtain Equation (8).

$$D := \frac{\sum_{i=1}^{\bar{N}} h_i \alpha_i}{v} \tag{7}$$

$$D = \frac{\bar{N} - 1}{\bar{N}} \tag{8}$$

Proposition 1. *In the homogeneous case, the dissipation ratio D is unaffected by changes in v. It is also unaffected by changes in α, as any changes in these two parameters will be offset by a proportional adjustment of h^*.*

However, D is a function of the number of potential miners $\bar{N}$. Intuitively this is a consequence of the increase in aggregate hash rate, $\bar{N}h^*$. In **Figure 1** we observe that an increase in $\bar{N}$ leads to an increase in aggregate expenditures.

Recall that individuals always have the outside option of $h_i = 0$. Consequently, the standard model will never deliver $D > 1$. A dissipation ratio >1 would mean that the total costs, caused by the allocation of mining resources, exceed the value of the reward—a rather unattractive business proposition. Thus, the dissipation ratio increases with $\bar{N}$, where $\lim_{\bar{N}\to\infty} D = 1$.

In the absence of any barriers to entry, potential miners will enter the market until the last bit of seigniorage is absorbed by the increasing hash rate.

Let us further denote network security as φ. As shown in Equation (9) we define network security as the minimum of all marginal costs multiplied by the network hash rate. In other words, φ is equivalent to the minimum cost an individual would have to bear to control half of the computation power and launch a surprise attack on the network. A surprise attack means that other miners are unaware of the imminent attack and hence, cannot adjust their resource allocations. Consequently, the larger the value for φ, the more expensive such an attack would be.

$$\varphi := \left[\min_{i\in N}\left(\frac{\alpha_i}{v}\right)\right] \sum_{i=1}^{\bar{N}} h_i^* \tag{9}$$

Although network security is an absolute measure that does not contain any information regarding efficiency, and although the dissipation ratio does not contain any information regarding network security, it can be shown that the two terms coincide under homogeneity assumptions.

Proposition 2. *Let there be $\bar{N} \geq 2$ homogeneous miners. Then, network security must be equal to the dissipation ratio $\varphi = D$.*

Proof. From (8) we know that $D = (\bar{N} - 1)/\bar{N}$. Starting with Equation (9), plugging in (4) and making use of miner homogeneity, we get

$$\varphi = \frac{(\bar{N} - 1)}{\bar{N}}, \text{ given } \alpha_i = \alpha, \forall i \in N.$$

Thus, $\varphi = D$. □

Consequently, an increase in the number of potential miners increases the dissipation ratio, drives down the expected payoffs, and ultimately leads to a seigniorage of 0. However, in the case of homogeneous miners we have shown that any expenditures positively affect network security φ to the same extent.

2.2. Heterogeneous Miners With $\bar{N} = 2$

Let us now relax the assumption of miner homogeneity. Instead we shall presume that there are different types of miners with varying marginal costs, $c_i(h_i, \alpha_i) = h_i\alpha_i$. These marginal costs are exogenously given and are represented by the vector $\boldsymbol{\alpha}$. The vector is of length $\bar{N}$ and includes $\alpha_i, \forall i \in N$. The variation may be the result of differences in operational costs or in access to mining equipment.

To keep our model simple, we will limit $\bar{N}$ to 2, although our numerical analysis has led to comparable results for $\bar{N} > 2$. Furthermore, we will assume that the variation is exclusively driven by differences in α_i (i.e., we will maintain our assumption that $v_i = v, \forall i$). The miners' utility functions can now be expressed as (10).

$$\pi_i(\boldsymbol{h}, \boldsymbol{\alpha}, v) = \frac{h_i}{h_i + h_{3-i}} v - \alpha_i h_i, \text{ with } i = \{1, 2\} \tag{10}$$

The first order conditions, solved for h_1^* and h_2^*, respectively, lead to the set of equations as given in (11).

$$h_i^* = \frac{\sqrt{h_{3-i}}\sqrt{v}}{\sqrt{\alpha_i}} - h_{3-i}, \text{ with } i = \{1, 2\} \tag{11}$$

The set of Equation (11) represents the optimal choices depending on the respective choice of the opponent h_{3-i}; the reward value, v; and the individual's marginal costs, α_i. In **Figure 2**, we have visualized the reaction curves.

Note, that we represent h in terms of v. Hence, a change in v will not cause the curves to shift. A change in α_i on the other hand, extends or compresses the respective curve. The dashed line represents an example of such a change, or more specifically, an increase of α_1. The intersection at the origin generally does not constitute a stable equilibrium. More precisely, $\boldsymbol{h} = \boldsymbol{0}$ becomes an equilibrium (and in fact the unique equilibrium), if and only if we are in the case of $v \leq 0$. Whenever there is a positive reward at stake, miners have an incentive to set $\boldsymbol{h} > \boldsymbol{0}$. For all $v > 0$, the equilibrium solution always incorporates two (or more) active miners, independent of the extent of the differences in their marginal costs.

Plugging one of the equations in (11) into the other and solving it for h_i yields Equation (12), which expresses the same maximization decision as a function of $\boldsymbol{\alpha}$. It is a more convenient

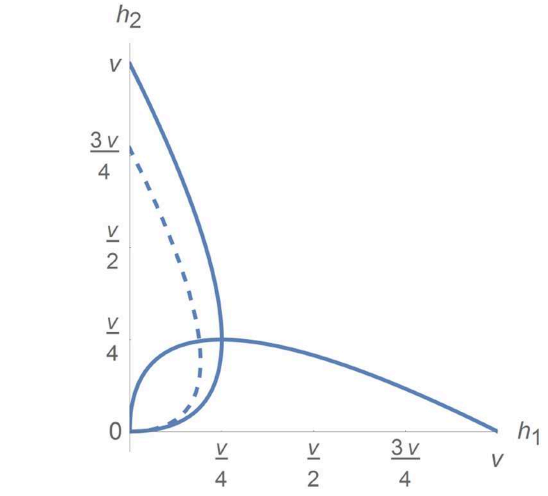

FIGURE 2 | Reaction curves from (11) with $\alpha_1 = \alpha_2 = 1$ and $\alpha_1 = 1.3$ (dashed).

expression of the optimal choice function as we have endogenized the opponent's hash rate decision.

$$h_i^* = \frac{v\alpha_{3-i}}{(\alpha_i + \alpha_{3-i})^2}, \text{ with } i = \{1, 2\} \tag{12}$$

To obtain Equation (13), an expression of the dissipation ratio, which is conditional on $\boldsymbol{\alpha}$ only, we can use (12) and plug it into (7).

$$D = \frac{2\alpha_1\alpha_2}{(\alpha_1 + \alpha_2)^2} \tag{13}$$

From (13) it can be shown, that the dissipation ratio decreases with miner heterogeneity. The first order derivative with respect to α_1 delivers Equation (14), which becomes negative if and only if $\alpha_1 > \alpha_2$. In this case an increase in α_1 is equivalent to an increase in heterogeneity.

$$\frac{\partial D}{\partial \alpha_1} = \frac{2\alpha_2(\alpha_2 - \alpha_1)}{(\alpha_1 + \alpha_2)^3} \tag{14}$$

However, the dissipation ratio contains no information on the extent of network security. In particular, a high dissipation ratio does not imply a high value for network security, φ, as it could instead be driven by a large number of highly inefficient miners. In such a case, the most efficient miner in the market could easily attack the network, despite the dissipation ratio being high. The network security on the other hand, has no explanatory power for the number of resources that have been spent to provide a certain value of φ.

Let us now combine the two, and introduce a measure, henceforth referred to as the security-efficiency ratio. It expresses the proportion of expenditures that serves to protect the network and hence, combines both the network's security and efficiency in one measure.

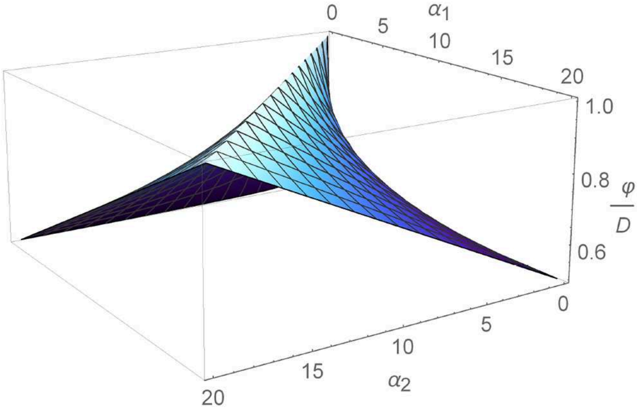

FIGURE 3 | $\frac{\varphi}{D}(\boldsymbol{\alpha})$ in the two-miner case.

As visualized in **Figure 3** and shown in the proof of Proposition 3, the security-efficiency ratio cannot exceed 1 and decreases with increasing heterogeneity. Furthermore, presuming $\bar{N} = 2$, it must lie in between $\frac{1}{2}$ and 1.

Proposition 3. *Let there be $\bar{N} = 2$ miners. Then, the security-efficiency ratio $\frac{\varphi}{D}$ decreases with relative heterogeneity and lies in the range of $\frac{\varphi}{D} = \left(\frac{1}{2}, 1\right]$.*

Proof. Plugging (12) into (9) and (13) and dividing (9) by (13), we get (15).

$$\min_{i=\{1,2\}} (\alpha_i) \frac{(\alpha_1 + \alpha_2)}{2\alpha_1\alpha_2} \tag{15}$$

Let us now assume without loss of generality that $\alpha_1 \geq \alpha_2$, such that $\min_{i=\{1,2\}} (\alpha_i) \equiv \alpha_2$. Through simplifying (15) we obtain (16).

$$\frac{\alpha_2}{2\alpha_1} + \frac{1}{2} \tag{16}$$

Case 1 ($\alpha_1 = \alpha_2$): As already shown in the proof of Proposition 2, presuming miner homogeneity, we get $D = \varphi$ and thus, $\frac{\varphi}{D} = 1$. This result can be easily replicated by using (16) and setting $\alpha_1 = \alpha_2$.

Case 2 ($\alpha_1 > \alpha_2$): Let us first consider the upper bound. By definition $\alpha_1 > \alpha_2$. Thus, values for $\frac{\varphi}{D}$ as shown in (16) must be smaller than 1. The relevant lower bound can be obtained by allowing the difference between α_1 and α_2 to get infinitely large, $\lim_{\frac{\alpha_2}{\alpha_1} \to 0}$. The first addend of Equation (16) then becomes infinitely small.

Thus, $\frac{\varphi}{D} \in \left(\frac{1}{2}, 1\right]$. □

Recall the homogeneous miners case, where we found $D = \varphi$ and hence, $\frac{\varphi}{D} = 1$. This is perfectly consistent with Proposition 3 and demonstrates how the network would benefit from miner homogeneity, assuming a potential attacker would be bound by the same parameters. Although perfect homogeneity would lead to a large dissipation ratio, the spent resources could not be classified as social waste in a broader sense, as they would positively impact network security. This means that although decentralization is strengthened by a higher number of miners, these participants should be as homogeneous as possible for efficiency reasons. Any market distortion (e.g., subsidies) will lead to a lower security-efficiency ratio.

2.3. Botnets and Homogeneous Miners

In the previous two sections, we limited our analysis to ordinary miners. Let us now consider a special type of miner whose marginal costs are larger than its expected marginal profits. Although puzzling at first, this type of miner may exist for a number of reasons including "hobbyists and researchers," "wishful thinkers," "botnet operators," "political actors," and "individuals looking for a virgin coinbase" (Swanson, 2014). In our analysis we will focus on botnets, but the following model could be used to describe situations with any of the actors described above.

The existence of botnets raises a couple of very interesting research questions for our analysis. First, is it possible that the dissipation ratio takes on values larger than 1? Recall that this means that miners as a whole consistently spend more than there is to gain. Likewise, what implications does the emergence of botnets have for network security, φ, and more importantly, for the security-efficiency ratio, $\frac{\varphi}{D}$?

To answer these questions, we extend our model and assume that there exists a botnet with $\bar{b} \geq 0$ units of hashing power, where $\bar{b}/(\bar{b} + \sum_i^{\bar{N}} h_i)$ represents the relative computation power of the botnet. For the sake of simplicity, we assume that the non-botnet miners are homogeneous with $\alpha_i = \alpha$, $\forall i \in N$ and further restrict $\bar{b} \leq \frac{\nu}{\alpha}$, as $\bar{b} = \frac{\nu}{\alpha}$ would be sufficient to crowd out any non-botnet miners. As we will see, these are reasonable assumptions. If a botnet obtained a relative hash rate even close to our restrictions, the network would be seen as corrupted and our analysis would be redundant.

Recall that an illegal botnet is a distributed pool of hardware resources (e.g., desktop computers) that have been taken over by a botnet operator. Botnets make use of the victims' computation and network resources. They carry out tasks, such as sending junk mail, click fraud to collect advertising revenues, and cryptocurrency mining. The botnet operator has a marginal cost of 0, as all the costs are borne by the actual owner of the resources. Consequently, we assume that botnets will always allocate the maximum amount of available resources, $\bar{b}$, to the hashing competition. We denote the average social cost per hash unit, as measured in (additional) electricity consumption and hardware depreciation, by α_b and restrict $\alpha_b > \alpha$. As mentioned before, these costs are borne by the owners of the infected computers.

As shown in Equation (17), we need to adjust the miners' expected payoff function by including the botnet's hash rate. Obviously, this has the effect of decreasing the miners' respective probabilities to win the competition and hence, has a negative impact on their expected payoff.

$$\pi_i^e(\boldsymbol{h}) := \frac{h_i \nu}{h_i + (\bar{N} - 1)h + \bar{b}} - \alpha h_i \tag{17}$$

We can now derive the first order condition with respect to h_i and presume non-botnet miner homogeneity. After a few more steps (shown in the **Supplementary Material**), we are able to solve for h in order to obtain Equation (18).

$$h^* = \frac{\nu(\bar{N} - 1) - 2\alpha\bar{b}\bar{N} + \sqrt{4\alpha\bar{N}^2(\bar{b}\nu - \alpha\bar{b}^2) + \left[\nu(\bar{N} - 1) - 2\alpha\bar{b}\bar{N}\right]^2}}{2\alpha\bar{N}^2} \tag{18}$$

Let us now turn to the efficiency analysis. The equation for the dissipation ratio must be slightly adjusted to (19), to include the social cost inflicted by the botnet.

$$D := \frac{\bar{b}\alpha_b + \bar{N}h^*\alpha}{\nu} \tag{19}$$

By using (18) we can eliminate h in (19) and re-express the equation, as shown in Equation (20).

$$D = \frac{2\bar{b}\bar{N}(\alpha_b - \alpha) + \nu(\bar{N} - 1) + \sqrt{4\alpha\bar{N}^2(\bar{b}\nu - \alpha\bar{b}^2) + \left[\nu(\bar{N} - 1) - 2\alpha\bar{b}\bar{N}\right]^2}}{2\bar{N}\nu} \tag{20}$$

The above expression allows us to demonstrate how the dissipation ratio changes in the presence of a botnet.

Proposition 4. *Let there be $\bar{N} \geq 1$ homogeneous miners and a botnet with $\bar{b} \in [0, \frac{\nu}{\alpha}]$ and $\alpha_b > \alpha$. Then, the dissipation ratio monotonically increases with $\bar{b}$ and lies in the set $\mathcal{D} = [\frac{\bar{N}-1}{\bar{N}}, \frac{\alpha_b}{\alpha}]$. If we add a strict inequality by assuming $\bar{b} > 0$, the dissipation ratio linearly increases with α_b and, for sufficiently large $\bar{N}$, is >1.*

Proof. Let us first show, that D linearly increases with α_b for all $\bar{b} > 0$. We derive (20) with respect to α_b to obtain (21). It can now be easily observed that D increases at a constant growth rate for all $\bar{b} > 0$, while it does not grow at all for the border cases with $\bar{b} = 0$.

$$\frac{\partial D}{\partial \alpha_b} = \frac{\bar{b}}{\nu} \tag{21}$$

Let us now analyze (20), considering different assumptions regarding $\bar{b}$ and show that $D \in \mathcal{D}$ for all $\bar{b} \in [0, \frac{\nu}{\alpha}]$.

Case 1 ($\bar{b} = 0$): If we presume $\bar{b} = 0$ we are back in the homogeneous miners case and can simplify Equation (20) until we get $D = \frac{\bar{N}-1}{\bar{N}}$, which corresponds to (8) and represents the lower bound of $\mathcal{D}$. As expected, this is consistent with the proof of Proposition 2.

Case 2 ($\bar{b} = \frac{\nu}{\alpha}$): If we set $\bar{b} = \frac{\nu}{\alpha}$, botnets are the sole source of hashing power in the network. Hence, the dissipation ratio is unaffected by $\bar{N}$. We can show this result by substituting $\bar{b}$ with $\frac{\nu}{\alpha}$

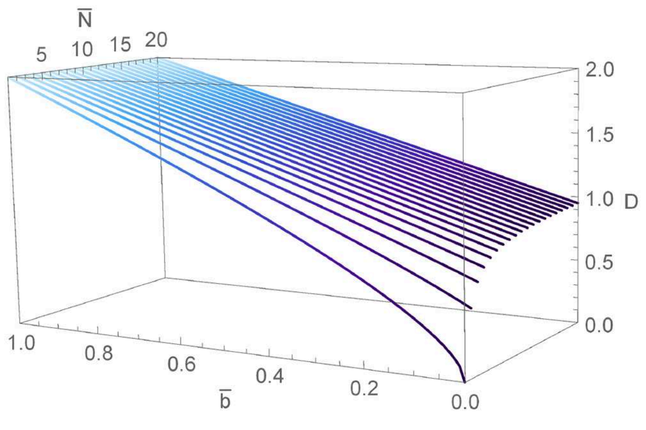

FIGURE 4 | $D(\bar{b}, \bar{N} | v = \alpha = 1, \alpha_b = 2)$.

in Equation (20). After a few simplification steps as shown in the **Supplementary Material**, we get $D = \frac{\alpha_b}{\alpha}$.[2]

Case 3 ($\bar{b} \in (0, \frac{v}{\alpha})$): In between the two border solution cases, it remains to be shown that $D \in \mathcal{D}$ for all $\bar{b} \in (0, \frac{v}{\alpha})$. Let us establish our proof by first looking at the change of D in $\bar{b}$. We derive (20) w.r.t. $\bar{b}$ and simplify the equation until we get (22).

$$\frac{\partial D}{\partial \bar{b}} = \frac{\alpha_b - \alpha}{\bar{N} v} + \frac{\alpha}{\sqrt{4\alpha^2 \bar{b} \bar{N}^2 \left(\frac{v}{\alpha} - \bar{b}\right) + \left[(\bar{N} - 1)v - 2\alpha \bar{b} \bar{N}\right]^2}} \tag{22}$$

The derivative shows, that D is monotonically increasing in $\bar{b}$ from our lower bound $\frac{\bar{N}-1}{\bar{N}}$, which must be smaller than 1, to our upper bound $\frac{\alpha_b}{\alpha}$, which by definition must be ≥1. Fitting all the pieces together, we know that for each $\bar{N}$, the border solutions are connected by a monotonically increasing path. This ensures that D will never exceed or undercut the border values, and hence, must always lie in $\mathcal{D}$. An example of this relationship with $v = \alpha = 1$ and $\alpha_b = 2$ is visualized in **Figure 4**.

Thus, $D \in \mathcal{D} = [\frac{\bar{N}-1}{\bar{N}}, \frac{\alpha_b}{\alpha}]$, which implies $\lim_{\bar{N} \to \infty} D \in [1, \frac{\alpha_b}{\alpha} \geq 1]$. □

As shown in the proof of Proposition 4, the presence of a botnet may cause the dissipation ratio to exceed 1. However, recall that the dissipation ratio is not a sufficient measure for our purposes, as it contains no information regarding the nature of the cost. In order to get an objective comparison, we need to reconsider the security-efficiency ratio, which was introduced earlier in this paper. Let us adjust Equation (9) to account for the botnet and divide it by (19) to obtain Equation (23).

$$\frac{\varphi}{D} = \frac{(\bar{b} + \bar{N} h^*)\alpha}{\bar{b}\alpha_b + \bar{N} h^* \alpha} \tag{23}$$

Plugging (18) into (23), we get (24), which expresses the security-efficiency ratio with endogenized hash rate allocation decisions.

$$\frac{\varphi}{D} = \frac{\bar{b}\alpha + \frac{\left(v(\bar{N}-1) - 2\alpha\bar{b}\bar{N} + \sqrt{4\alpha\bar{N}^2(\bar{b}v - \alpha\bar{b}^2) + \left[v(\bar{N}-1) - 2\alpha\bar{b}\bar{N}\right]^2}\right)}{2\bar{N}}}{\bar{b}\alpha_b + \frac{\left(v(\bar{N}-1) - 2\alpha\bar{b}\bar{N} + \sqrt{4\alpha\bar{N}^2(\bar{b}v - \alpha\bar{b}^2) + \left[v(\bar{N}-1) - 2\alpha\bar{b}\bar{N}\right]^2}\right)}{2\bar{N}}} \tag{24}$$

Equations (23) and (24) both show that the security-efficiency ratio must be 1 whenever $\bar{b} = 0$ and/or $\alpha_b = \alpha$.

Proposition 5. *Let there be $\bar{N} \geq 1$ homogeneous miners and a botnet with $\bar{b} \in [0, \frac{v}{\alpha}]$ and $\alpha_b \geq \alpha$. Then, the security-efficiency ratio must c.p. monotonically decrease with $\bar{b}$ and α_b. Moreover, it must lie in $\frac{\varphi}{D} \in [\frac{\alpha}{\alpha_b}, 1]$.*

Proof.

Case 1 ($\bar{b} = 0$): For $\bar{b} = 0$ and/or $\alpha_b = \alpha$, the numerator and denominator in Equation (23), or alternatively in (24), must be equal. As a result, we get our upper bound which corresponds to $\frac{\varphi}{D} = 1$.

Case 2 ($\bar{b} = \frac{v}{\alpha}$): For $\bar{b} = \frac{v}{\alpha}$ we can reduce Equation (24) until we get $\frac{\varphi}{D} = \frac{\alpha}{\alpha_b}$. This corresponds to the case with $h^* = 0$ in Equation (23), as any non-botnet miners would be crowded out by the botnet. If both $\bar{b} > 0$ and $\alpha_b > \alpha$ are satisfied, the numerator will always be smaller than the denominator, with

$$\frac{\partial \frac{\varphi}{D}}{\partial \alpha_b} < 0; \frac{\partial \frac{\varphi}{D}}{\partial \bar{b}} < 0.$$

Thus, $\frac{\varphi}{D} \in [\frac{\alpha}{\alpha_b}, 1]$. □

Figure 5 shows the effects of a botnet, depending on the initial number of miners in the market. In the left-hand figure we have a mining market with $\bar{N} = 2$. Hence, a botnet causes an immediate drop in $\frac{\varphi}{D}$. In the right-hand figure we observe a market with $\bar{N} = 20$. Here, the drop in $\frac{\varphi}{D}$ due to a change in α_b is mitigated, as most of it occurs only if the botnet is able to take over a certain portion of the network.

The observed change for crowded miner markets can be explained by the consideration of the crucial difference in the parameters $\bar{b}$ and α_b. Note that $\bar{b}$ is an expression for hashing power provided by the botnet, and hence, influences all the optimal choice functions. Accordingly, a change in $\bar{b}$ leads to a change in the allocation vector of the non-botnet miners, $\boldsymbol{h}$, conditional on $\bar{N}$. The parameter α_b on the other hand, is an expression of cost borne by society, which does not influence any of the individual hash rate allocation decisions. Since $\alpha < \alpha_b$, the measure for network security, φ, is also unaffected by any changes in α_b. Instead, α_b exclusively influences D. In particular, an increase in α_b must c.p. lead to a linear increase in D. Recall

[2] Note that it theoretically is possible to get $\bar{b} > \frac{v}{\alpha}$. In such a case we would need to consider the non-negativity constraint $h_i \geq 0, \forall i$ in order to reduce the dissipation ratio equation to $D = \frac{\bar{b}\alpha_b}{v} > \frac{\alpha_b}{\alpha}$. However, this means that the (inefficient) botnet allocates more hashing power than the (efficient) miners would in a perfect competition equilibrium. We decided to mention this case in a side note, because it seemed to be very unlikely.

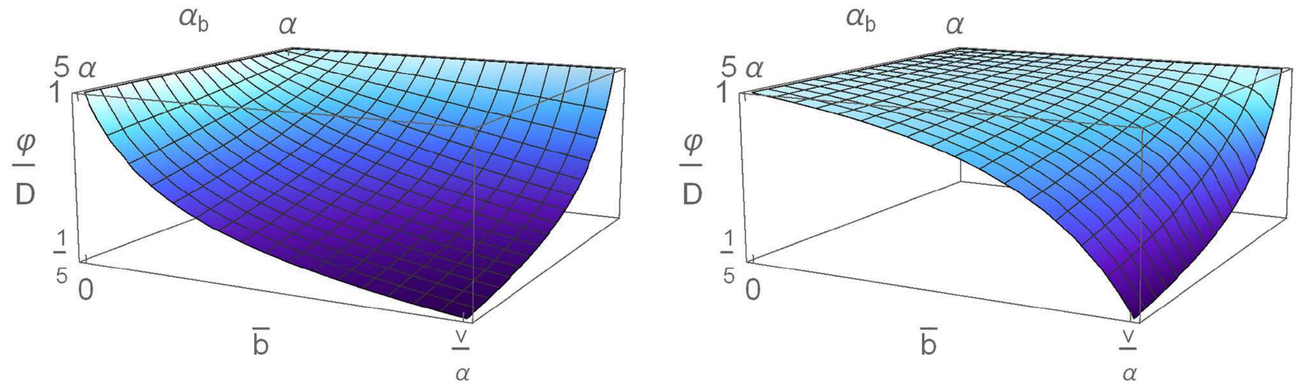

FIGURE 5 | $\frac{\varphi}{D}(\bar{b}, \alpha_b)$ with $\bar{N} = 2$ and $\bar{N} = 20$.

that this has been shown in the proof of Proposition 4. The linearly growing denominator, in turn, must c.p. lead to a convex decrease in $\frac{\varphi}{D}$. Thus, the larger the initial dissipation ratio, the less significant the increase. Taking into account the effects of $\bar{N}$ on D, it becomes apparent, that α_b has a larger effect on $\frac{\varphi}{D}$, in low $\bar{N}$ markets.

3. CONCLUSION

We have proposed a model that allows for the evaluation of the efficiency of proof-of-work mining under different circumstances by categorizing the allocated resources as either useful or wasteful. The model also shows how security and efficiency are affected by miner heterogeneity. To relate those two values, we proposed the security-efficiency ratio, a value that expresses the portion of the aggregate expenditures that is used to secure the blockchain. We then showed that the security-efficiency ratio decreases with increasing miner heterogeneity. Any market distortion that increases miner heterogeneity will lower the security-efficiency ratio.

Additionally, we demonstrated how the introduction of a botnet affects the network. We concluded that botnets decrease the security-efficiency ratio and may even lead to dissipation ratios above 1. Consequently, systems that are more susceptible to botnet capture, such as ASIC-resistant proof-of-work implementations, may be more prone to these inefficiencies under the assumption that all other hashrate providers face the same cost.

This model is presented as a framework for future studies with questions regarding the efficiency of proof-of-work mining.

DATA AVAILABILITY STATEMENT

All datasets generated for this study are included in the article/**Supplementary Material**.

AUTHOR CONTRIBUTIONS

The author confirms being the sole contributor of this work and has approved it for publication.

SUPPLEMENTARY MATERIAL

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fbloc.2020.00016/full#supplementary-material

REFERENCES

Berentsen, A., and Schär, F. (2017). *Bitcoin, Blockchain und Kryptoassets*. Norderstedt: Books on Demand.

Berentsen, A., and Schär, F. (2018). A short introduction to the world of cryptocurrencies. *Fed. Reser. Bank St. Louis Rev.* 100, 1–16. doi: 10.20955/r.2018.1-16

Dimitri, N. (2017). Bitcoin mining as a contest. *Ledger* 2, 31–37. doi: 10.5195/ledger.2017.96

Nakamoto, S. (2008). *Bitcoin: A Peer to Peer Electronic Cash System*. Available online at: https://www.bitcoin.com/bitcoin.pdf (accessed January 18, 2018).

O'Dwyer, K. J., and Malone, D. (2014). *Bitcoin Mining and Its Energy Footprint*. Limerick: IET.

Sams, R. (2014). *The Marginal Cost of Cryptocurrency*. Available online at: http://www.cryptonomics.org/2014/01/15/the-marginal-cost-of-cryptocurrency/ (accessed January 18, 2018).

Swanson, T. (2014). *The Anatomy of a Money-Like Informational Commodity: A Study of Bitcoin*. Available online at: https://s3-us-west-2.amazonaws.com/chainbook/The+Anatomy+of+a+Money-like+Informational+Commodity.pdf (accessed January 18, 2018).

Tullock, G. (1980). "Efficient rent-seeking," in eds J. M. Buchanan, R. D. Tollison, and G. Tullock *Toward a Theory of the Rent-Seeking Society*. College Station, TX: Texas A&M University Press, 3–15.

Conflict of Interest: The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.