ELIMINATING ENVIRONMENTAL COSTS TO PROOF-OF-WORK-BASED CRYPTOCURRENCIES: A PROPOSAL

Gabriel Mathy [*]
American University

December 22, 2022

Abstract

The process of mining Bitcoin consumes an enormous amount of electricity. This is an inherent feature of the way that Proof-of-Work based cryptocurrencies work today. While there are more environmentally friendly alternatives, like Proof-of-Stake, these have their own drawbacks. Instead, this paper proposes an alternative algorithm for Bitcoin that would reduce the electricity usage on the order of trillions. Rather than adjusting the difficulty of Bitcoin mining upward when more miners are devoting computing power to mining, the returns to mining would be reduced downwards. This would be done one of two ways: either by reducing the amount of Bitcoin awarded to miners, or by altering the algorithm governing wallets to scale up or down the amount of Bitcoin outstanding to lower the price of Bitcoin. Rather than the current situation where Bitcoin's difficulty is in the trillions, by reducing the reward to mining, the mining difficulty could be set to the theoretical minimum, 1. This would reduce the electricity usage of Bitcoin by a factor of trillions. The paper concludes with a discussion of a mechanism to avoid 51% attacks and of the implications of this proposal for the take-up of Bitcoin and other Proof-of-Work based cryptocurrencies.

JEL Codes: D02, Q30, Q40

Keywords: Bitcoin, Environmental Costs of Cryptocurrencies, Mechanism Design

[*] Address: 4400 Massachusetts Avenue, Washington, DC 20016. E-mail: mathy@american.edu. Phone: +1.202.885.3708. The paper has benefited significantly from feedback from two anonymous referees and the editors.

1 Introduction

Proof-of-Work (POW) mechanisms, such as those used by Bitcoin, require a huge amount of electricity (Vranken, 2017). Proof-of-Stake (POS) mechanisms provide a promising alternative, with minimal computational requirements, which reduce electricity use (Saleh, 2021). There are drawbacks to POS however, including lessened security, the influence of large players, and illiquidity when staking. This paper proposes a market-based mechanism that will provide all the benefits of POW without any of the environmental costs, with electrical usage as low, or lower, than a POS mechanism. POW mechanisms are based on the solution to cryptographic problems, which are difficult to solve but trivially easy to verify. Miners that successfully solve these difficult cryptographic problems are allowed to add transactions to the blockchain through the formation of new blocks. I will consider the case of Bitcoin, as the most famous cryptocurrency (Velde, 2013). POW mechanisms vary in their specifics, but the general principles remain the same across all POW-based cryptocurrencies.

New block formation creates a permanent and indelible record of cryptocurrency transactions which can be viewed by anyone on the planet. The time required for new block formation, or the "block time", will vary based on the amount of computing power in the system. If block time is too short, then fewer transactions will be added to each block, making it potentially less secure. If the block time is too long, then transactions are added infrequently and this delay is inconvenient for those trying to use Bitcoin for transactions. There is no single optimal block time. Bitcoin's algorithm currently forms blocks ever ten minutes. However, whatever block time is chosen, currently, all cryptocurrencies that use POW adjust the difficulty of mining a block to delay and accelerate block formation (Kraft, 2016). This functions as a tax of sorts (Podhorsky, 2021). While difficulty is part of the security aspect of the chain and cannot be eliminated entirely, increasing the difficulty does not improve any other aspect of Bitcoin's functioning and simply makes mining use more electricity than it would if the difficulty were lower. Increasing difficulty involves a pure waste of electricity, and is the primary reason why Bitcoin mining uses so much electricity.

As interest in Bitcoin has grown and the price of Bitcoin has risen, difficulty has increased, reaching a difficulty in the trillions today. However, this is not the only way to ensure that block time hits a target. This paper proposes an alternative mechanism. Instead, the quantity of outstanding cryptocurrency would be scaled downward until the price of Bitcoin would be adjusted downward, or the amount of Bitcoin awarded to new miners would be adjusted downward, until miner interest declines. This would ensure a constant block time, and so difficulty could be set to its technological minimum at 1.

This would reduce the electricity usage by Bitcoin on the order of trillions, resulting in an electricity usage far below that of the formal banking and financial system. This change would eliminate environmental concerns with Bitcoin. The differences between the two protocols, the current one, and the new one proposed in this paper, are derived formally using a microeconomic model of miner profit maximization. Some tradeoffs involved with having algorithmic quantity adjustment rather than algorithmic difficulty adjustment are also discussed, as well as a method to avoid 51% attacks, where a large enough miner could effectively take-over the Bitcoin network and post fraudulent transactions. Then, the paper concludes.

2 Model

There are many models of the economics of Bitcoin and cryptocurrencies (Dwyer, 2015; Cocco and Marchesi, 2016; Schilling and Uhlig, 2019), and a model will be useful to demonstrate how this alternative mechanism works.

2.1 Quantities

The time period is given by t. The aggregate quantity of Bitcoin at any period t is given by Q_t, with the following law of motion:

$$Q_{t+1} = \Delta Q_t + Q_t \tag{1}$$

Each individual miner is indexed by $j \in \mathbb{N}$. As in Prat and Walter (2021), we will assume that there is free entry in this decentralized market for mining. The quantity of Bitcoin awarded to the jth miner, G_t^j, is proportional to the amount of Bitcoin being created with each block, ΔQ_t.

$$G_t^j = \alpha'_{Q,t} \Delta Q_t \tag{2}$$

Miners can also be awarded a block fee as a side payment. These are offered by those wanting to be at the front of the queue to be placed on the next block. These block fee per transaction will be referred to as B_t, with the number of transactions referred to as D_t. Due to the competition among miners, B_t will be the same for all miners, and will not carry a j subscript. This paper is not concerned with the determination of these block fees, which are based on transaction demand for Bitcoin. For simplicity, the block fees will be denoted in units of Bitcoin, more specifically in units of the change in Bitcoin, such that

$$D_t B_t = \alpha''_{Q,t} \Delta Q_t \tag{3}$$

For simplicity, then, the scalars will sum to an aggregate scalar, α_Q :

$$\alpha_{Q,t} = \alpha'_{Q,t} + \alpha''_{Q,t} \tag{4}$$

The total amount of Bitcoin awarded to a miner for successful hashing, A_t^j, is:

$$A_t^j = G_t^j + D_t B_t = \alpha'_{Q,t} \Delta Q_t + \alpha''_{Q,t} \Delta Q_t = \alpha_{Q,t} \Delta Q_t \tag{5}$$

2.2 Computing Power

Cryptographic hashing involves devoting a certain amount of computing power to solving the cryptographic problems. These are difficult to solve but trivial to verify. The cryptographic difficulty is given by D_t, in units of hashes. This difficulty linearly increases the difficulty of solving the cryptographic hash and similarly linearly reduce the probability of solving the mining successfully. There is some probability, p_t, of solving the cryptographic exercise, which is proportional to the amount of computing power devoted to mining by the jth miner, and which is proportional to the difficulty D_t, following scalar α_p. The computing power devoted to mining by the jth miner is M_t^j, in units of hashes.

$$p_t = \alpha_p \frac{M_t^j}{D_t} \tag{6}$$

There are two states: Either hashing is successful, in which case the miner is awarded a certain amount of Bitcoin, or is unsuccessful, in which case the miner receives nothing. The expected reward, Z_t^j, is thus

$$Z_t^j = E_t[p_t A_t^j + (1 - p_t)0] = E_t[p_t A_t^j] = E_t\left[\alpha_p \frac{M_t^j}{D_t} \alpha_Q \Delta Q_t\right] \tag{7}$$

2.3 Time and Computing Power

The time between the formation of new blocks for the jth miner is given by a^j, with the target time between blocks being formed denoted by a^*. The target is the same for all blocks, though it may vary across miners. The time between block formation is inversely proportional to the total computing power devoted to mining, M_t^j, and proportionally related to difficulty:

$$a_t^j = \alpha_a^j \frac{D_t}{M_t^j}$$

The optimal block formation time, a^*, is simply the mean of the individual block formation times,

$$a_t^* = \frac{1}{N} \sum_{j=1}^{N} a_t^j = \frac{1}{N} \sum_{j=1}^{N} \alpha_a^j \frac{D_t}{M_t^j} \tag{8}$$

For the Bitcoin protocol to have a set time to form blocks, the amount of computing power in the system must be set to the appropriate level. This is done by adjusting difficulty every 2016 blocks, which is roughly ever two weeks. Difficulty is adjusted up is block formation time is too low, and is adjusted down is block formation time is too high. The electrical needs in kilowatt-hours required to run the computers mining Bitcoin is given by E_t^j. The electrical costs are proportional to the amount of computer power devoted to mining, M_j, following:

$$E_t^j = \alpha_E M_t^j$$

where α_E is the amount of electricity used for a single hash. Here it will be assumed that this does not vary across miners for simplicity, though this could be relaxed. We can then sum over all j miners, obtaining

$$E_t = \sum_{j=1}^{N} E_t^j = \sum_{j=1}^{N} \alpha_E M_t^j = \alpha_E M_t \tag{9}$$

This implies that the amount of electricity is proportional to the amount of computing power devoted to mining (in hashes).

2.4 Miner Costs

The cost for a miner of mining one Bitcoin is C_t^j, measured in U.S. dollars. The cost of electricity will be assumed to follow a quadratic cost function, which is a commonly assumed cost structure for electricity generation (Martínez-Budría et al., 2003; Cain and Alvarado, 2004; Jara-Dıaz et al., 2004; Qiu et al., 2009; Fetz and Filippini, 2010). There will be fixed costs, such as structures to house mining operations, denoted by F^j. There will be the linear cost of electricity, L^j, multiplied by their use of electricity, E_t^j, and a quadratic cost of electricity, T^j, multiplied by the square of the use of electricity by the jth miner, following

$$C_t^j = F^j + L^j E_t^j + T^j (E^{j_t})^2 = F^j + L^j \alpha_E M_t^j + T^j (\alpha_E M_t^j)^2. \tag{10}$$

The marginal cost of mining will thus be the price of electricity, L^j, multiplied by the amount of electricity used for a single hash, α_E, plus double the quadratic cost, $2T^j$, multiplied by the square of α_E multiplied by the amount of computing power devoted by miner j.[1] The miners with the lowest electricity costs will operate when the returns to mining are low, and miners with higher electricity costs will enter the market as the return to mining increases.

2.5 Miner Revenue

The price of Bitcoin is given by P_t. The expected revenue from mining, R_t, is assumed to follow the statistical expectation with respect to time, $E_t[]$, and is the product of the probability of success, the quantity of Bitcoin awarded, and the price of Bitcoin, given by:

$$E_t[R_t] = E_t[Z_t P_t] = E[p_t A_t P_t] = E_t\left[\alpha_p(\alpha_{Q,t}\Delta Q_t)\frac{M_t}{D_t}P_t\right] = \alpha_p(\alpha_{Q,t}\Delta Q_t)\frac{M_t}{D_t}E_t\left[P_t\right] \tag{11}$$

We will assume the price of Bitcoin is fixed in any given period, and thus obtain:

$$E_t[R_t] = \alpha_p(\alpha_{Q,t}\Delta Q_t)\frac{M_t}{D_t}P_t. \tag{12}$$

2.6 Miner Profit

Profits, Π_t^j, are the difference between miner revenues, R_t^j, and miner costs, C_t^j, following:

$$\Pi_t^j = R_t^j - C_t^j \tag{13}$$

There is no uncertainty over costs once the decision of how much computing power to devote to mining is taken, yielding

[1] If the α_E parameter were to vary across miners, it would be isomorphic to variations in the price of electricity across miners.

$$E_t[\Pi_t^j] = E_t[R_t^j - C_t^j] = E_t[R_t^j] - E[C_t^j] = \alpha_p(\alpha_{Q,t}\Delta Q_t)P_t\frac{M_t^j}{D_t} - F^j - L^j\alpha_E M_t^j - T^j(\alpha_E M_t^j)^2$$

or

$$E[\Pi_t^j] = M_t^j\left(\alpha_p(\alpha_{Q,t}\Delta Q_t)P_t\frac{1}{D_t} - L^j\alpha_E - M_t^j T^j(\alpha_E)^2\right) - F_t^j \tag{14}$$

2.7 Profit Maximization

Miners will maximize profits by choosing computer power to devote to mining, following:

$$argmax_{M_j}E[\Pi_t^j] = argmax_{M_j}\left[M_t^j\left(\alpha_p(\alpha_{Q,t}\Delta Q_t)P_t\frac{1}{D_t} - L^j\alpha_E - M_t^j T^j(\alpha_E)^2\right) - F_t^j\right] \tag{15}$$

The optimal choice of computer power for the jth miner is thus

$$0 = \alpha_p(\alpha_{Q,t}\Delta Q_t)P_t\frac{1}{D_t} - L^j\alpha_E - 2M_t^{j*}T^j(\alpha_E)^2$$

which can be rewritten as:

$$M_t^{j*} = \frac{1}{2T^j(\alpha_E)^2}\left(\alpha_p(\alpha_{Q,t}\Delta Q_t)P_t\frac{1}{D_t} - L^j\alpha_E\right) \tag{16}$$

The reader will recall that the gross computing power devoted to mining is M_t. This is also the sum of all the individual miners devoting computing power to hashing, or

$$M_t = \sum_{j=1}^{N} M_t^j \tag{17}$$

Which results in the optimal aggregate computing power, M_t^*, being:

$$M_t^* = \sum_{j=1}^{N} \frac{1}{2T^j(\alpha_E)^2} \left(\alpha_p(\alpha_{Q,t}\Delta Q_t)P_t \frac{1}{D_t} - L^j \alpha_E \right)$$

or

$$M_t^* = \frac{1}{2\alpha_E} \left(\frac{\alpha_p \alpha_{Q,t} \Delta Q_t P_t}{2D_t(\alpha_E)} \sum_{j=1}^{N} \frac{1}{T^j} - \sum_{j=1}^{N} \frac{L^j}{T^j} \right) \tag{18}$$

This will characterize the optimal choice of computing power for the firms operating in the market. Only firms that are profitable will mine, while those that are unprofitable will exit, so the N firms will be composed of the firms which are profitable.

3 Potential Bitcoin procotols

3.1 Current framework

Next we outline the current framework for Bitcoin. The path of Bitcoin is fixed in advance, such that the growth rate of Bitcoin is nonnegative but declines periodically.[2] The growth rate will eventually fall to zero around the year 2140 and will asymptotically approach 21 million Bitcoin issued in total. This implies that the amount of Bitcoin outstanding at any time is fixed in advance, following

$$Q_t = \overline{Q_t}. \tag{19}$$

This implies that the new issuance of Bitcoin is also fixed.

$$\Delta Q_t = \overline{\Delta Q_t}. \tag{20}$$

Let's return to the profit maximizing equation, Equation 16, which in this case is:

[2] The original issuance was 50 Bitcoin per block, but this growth rate is cut in half after every 210,000 blocks are mined.

$$M_t^* = \frac{1}{2\alpha_E}\left[\left(\frac{\overline{\Delta Q_t}}{D_t^*}\right)\frac{\alpha_p \alpha_{Q,t} P_t}{2(\alpha_E)}\sum_{j=1}^{N}\frac{1}{T^j} - \sum_{j=1}^{N}\frac{L^j}{T^j}\right] \tag{21}$$

The difficulty is set to induce miners to not devote as much computing power to the system if the return to mining rise with the price of Bitcoin. As we can see above, if we assume the cost conditions for miners mining do not change, the difficulty will be proportional to the price of Bitoin. As the price of Bitcoin rises, the return to mining increases, which would reduce the time to form blocks. In response, the algorithm increases the difficulty, to make it more expensive to mine, and wasting electricity, which serves no good purpose.

3.2 Alternative Proposal

Next we consider an alternative framework, where the return to mining will be adjusted downward in the face of increased computing power devoted to hashing, to allow for block formation at the required time, rather than difficulty being adjusted upward as is the status quo. This would involve scaling the amount of new Bitcoin introduced, ΔQ_t, according to

$$\Delta Q_t^* = \alpha_s \Delta Q_{t-1}, \tag{22}$$

where α_s is an arbitrary scalar, which is a positive, real number, and one time period is defined as one block unit of block time. α_s would be increased if the desired return to mining should be increased, and decreased if the desired reward to mining should be decreased. Difficulty would be set to 1, the technical minimum. If the reduction in difficulty to 1 were done in isolation, time to mine a block would become instantaneous, as there would be high return to mining Bitcoin, while cryptographic difficulty would be trivial and so mining would be easily successful. To offset this, the return to mining should be reduced by reducing the amount of Bitcoin awarded for mining, rather than by increasing the difficulty of mining.

Equation 21 becomes

$$M_t^* = \frac{1}{2\alpha_E}\left[\left(\frac{P_t^*(Q_t)\Delta Q_t^*}{D_t^*}\right)\frac{\alpha_p \alpha_{Q,t}}{2(\alpha_E)}\sum_{j=1}^{N}\frac{1}{T^j} - \sum_{j=1}^{N}\frac{L^j}{T^j}\right] \tag{23}$$

where now the quantities awarded to miners, ΔQ_t^*, can be adjusted to his the target of M_t^*, rather than the difficulty, D_t, which is set to 1. We would expect that the price of Bitcoin might be affected by changes in the quantity, and so this also needs to be chosen optimally.

There would be two sources of demand. The first would stem from investors that view the cryptocurrency as an asset. For these investors, scaling the quantity of cryptocurrency up would be equivalent to a dividend, and would tend to increase demand for this asset. The other source of demand would come from those who use the cryptocurrency for transactions, and so view the cryptocurrency as money. there they would have a traditional demand curve. In that case, scaling the quantity up would increase the supply available, moving them along their demand curve for the cryptocurrency as money.

The literature tends to support that more market participants view Bitcoin as an asset rather than money (Briere et al., 2015; Yermack, 2015; Baur et al., 2018; Sharma et al., 2019; Baur and Dimpfl, 2021; Mattke et al., 2021). That would imply that the scaling parameter, α_s, should be less than one in cases when mining interest increases, which will reduce demand. However, if this generates increases in demand, the algorithm could switch to a strategy of moving the scaling parameter to be greater than 1. These adjustments should be made every time a block is mined in order to ensure that block times stay roughly constant.

I will assume that the elasticity is fairly constant over the range of quantities of Bitcoin under consideration, or this can be taken as an approximation of the average elasticity over the changes in quantities. This elasticity is given by ε_d, and the demand curve for Bitcoin will be:

$$Q = \alpha_D P^{\varepsilon_d} \tag{24}$$

where α_D is a positive real number, but which will be normalized to 1 for simplicity. Defining ΔP in a similar fashion as ΔQ as

$$\Delta P = P_t - P_{t-1}$$

then we can relate the percent changes in quantities to the percent changes in prices as

$$\frac{\Delta Q}{Q} = \varepsilon_d \frac{\Delta P}{P} \tag{25}$$

by taking log differences of Equation 24. Rearranging results in

$$P^* = \varepsilon_d \frac{Q \Delta P}{\Delta Q}. \tag{26}$$

Plugging in Equation 26 into Equation 23 results in

$$M_t^* = \frac{1}{2\alpha_E} \left[\left(\frac{Q_t^* \Delta P^*}{D_t^*} \right) \frac{\alpha_p \alpha_{Q,t}}{2(\alpha_E)} \sum_{j=1}^{N} \frac{1}{T^j} - \sum_{j=1}^{N} \frac{L^j}{T^j} \right] \tag{27}$$

where ΔP^* is implied by Q_t^* and ε_d .

Given that the change in new Bitcoin awarded is generally small relative to the stock of Bitcoin outstanding ($\Delta Q < Q$), we can expect that the change in the reward, Z, will mostly be driven by changes in the amount of new Bitcoin awarded. If prices rise in response to a reduction in the new Bitcoin awarded to miners, then the reward will need to be reduced more to keep block formation time constant, so ΔQ will need to be reduced more in that case. However, as ΔQ approaches zero, the reward to new mining gets very small, so this should reduce computing power to a low enough level to hit any target for block formation time.

In practice, this target would be hit using a type of tâtonnement process , similar to what is used currently by the Bitcoin protocol. Under the status quo, difficulty is adjusted upward or downward periodically, corresponding to block formation time which is lower or higher than the target. Under this alternative, the quantity of Bitcoin awarded would be adjusted downward or upward instead. This would involve changing the code governing the Bitcoin protocol, which would require a consensus, just like any other change to

Bitcoin's code.

3.3 Changing quantity directly

Another option would be to adjust the quantity of Bitcoin itself, rather than adjusting the new Bitcoin awarded to miners. In this case, the amount of Bitcoin awarded to miners would be the same as the status quo. Instead, the code governing the blockchain would be changed so that all Bitcoin holdings in existing wallets could be scaled up or down proportionally, following:

$$Q_t = \alpha_{s'} Q_{t-1} \tag{28}$$

This would likely be viewed very negatively by those facing a shrinking of the quantity of Bitcoin they hold. However, this would be a feasible alternative which would allow for block formation time to be stabilized while setting difficulty to the minimum of 1. We would still have a similar formulation for the optimal amount of computing power (in hashes):

$$M_t^* = \frac{1}{2\alpha_E} \left[\left(\frac{Q_t^* \Delta P^*}{D_t^*} \right) \frac{\alpha_p \alpha_{Q,t}}{2(\alpha_E)} \sum_{j=1}^{N} \frac{1}{T^j} - \sum_{j=1}^{N} \frac{L^j}{T^j} \right] \tag{29}$$

However, the elasticity of demand could be quite different if we are adjusting the quantity of all Bitcoin oustanding, Q_t, by scaling Bitcoin in existing wallets. If the margin is having a bit more or less additional Bitcoin from new mining, as above, then a standard demand curve would result. However, if the existing quantity is reduced, that introduces the prospect of capital losses, which would reduce demand. However, if Bitcoin is used in transactions, then Bitcoin holders may demand more Bitcoin in this case, to return to holding a target level of Bitcoin to engage in transactions. Thus the slope of the demand curve will depend on whether demand is driven by the desire to hold Bitcoin as a speculative asset, or in order to perform transactions.

The literature tends to support that more market participants view Bitcoin as an asset rather than money (Briere et al., 2015; Yermack, 2015; Baur et al., 2018; Sharma et al., 2019; Baur and Dimpfl, 2021; Mattke et al., 2021). That would imply that changes in quantities are positively correlated with changes in prices, so that a reduction in quantities (by scaling down existing wallets) would also lower the price, as asset returns would be negative. This implies that the elasticity of demand is, somewhat perversely, positive, and so reducing the total quantity of Bitcoin outstanding will reduce the price, and thus reduce the return to mining, even if the quantity of new Bitcoin issued remains fixed.

The scaling parameter, $\alpha_{s'}$, should be less than one in cases when mining interest increases, which will reduce demand. However, if this generates increases in demand, the algorithm could switch to a strategy of moving the scaling parameter to be greater than 1. These adjustments should be made every time a block is mined in order to ensure that block times stay roughly constant. Given the prospect for capital losses, it is expected that the first proposal will be preferred, though this mechanism is feasible too.

At the time of writing, difficulty is approximately 37 trillion, near a record high.[3] Since the difficulty is proportional to electricity use, by setting the difficulty to 1, the electricity use would be cut by a factor of 37 trillion, or $3.7^{*}10^{13}$. Bitcoin's electricity usage is estimated to be about 11 Gigawatts, annualized to 94 terawatt-hours. Using this alternative approach would reduce the electricity usage by Bitcoin annually to 2.5 watt-hours, less than the electricity required to run a standard LED lightbulb for about ten minutes.[4] This change would effectively eliminate the electricity usage of Bitcoin and, so, would eliminate the environmental concerns associated with Bitcoin and other POW cryptocurrencies. If a difficulty of 1 too low a level and so it would be trivially easy to overload the network, then the difficulty can be set higher while still allowing electricity usage to be trivially small from an environmental perspective.

[3] Source: https://www.blockchain.com/charts/difficulty, accessed November 22nd, 2022.

[4] Source: https://ccaf.io/cbeci/index, accessed June 8th, 2022

4 A Fundamental Trade-off: Widespread Use or Attractive Asset?

This section discusses some fundamental trade-offs for a cryptocurrency like Bitcoin. The most fundamental one is the tradeoff between widespread adoption of Bitcoin and Bitcoin being an attractive asset, with a price that tends to go up over time. The current set-up has favored the latter, with a rigid rule that introduces relatively little Bitcoin, with the growth rate slowing over time. While this was implemented to avoid the hyperinflationary possibilities of an electronic currency with no inherent scarcity, this created almost completely inelastic supply conditions for Bitcoin. As a result, increased desire to participate in the Bitcoin ecosystem generated strong increases in price, further fueling enthusiasm in Bitcoin as an attractive asset experiencing strong capital gains.

However, under the current framework for Bitcoin, increased mining activity resulted from an increased desire to hold Bitcoin. This increased the costs to mining, both for the pocketbook and the environment. For buyers, high price volatility and periodic sudden declines in price increased risk, making Bitcoin very risky, as opposed to most monies, which are very safe. This impedes Bitcoin's takeup as money used widely across the globe, limiting its use primarily to those interested in alternatives to formal banking and financial systems or those interested in investing in Bitcoin as an asset.

Using algorithmic adjustment to the quantity of Bitcoin, both outstanding and being awarded to miners, rather than the current difficulty-based approach, would allow Bitcoin to find much wider acceptance. However, this would come at the cost of making it very unattractive as an asset. As interest in Bitcoin increased, then the price would be driven lower through a reduction in Bitcoin outstanding, and the awards to miners would be reduced. This would allow for increasingly ever affordable Bitcoin, with anyone on the planet able to mine Bitcoin.

This has to potential to make Bitcoin a truly revolutionary type of money, which is accessible to anyone on the planet at a trivial cost, with essentially no environmental impact. However, there would come at the cost that interest in Bitcoin as a asset would be decimated, as Bitcoin would tend to experience capital losses. One would expect that, rather than the current situation, where Bitcoin is held as an attractive investment, that Bitcoin holders would attempt to liquidate their holdings as soon as possible to avoid capital losses. This is a fundamental, intractable trade-off. Current Bitcoin supporters who believe that Bitcoin is an ideal financial investment, while simultaneously believing that Bitcoin is the future of money can only be half right. They need to pick which one will be the case, and for the moment, the Bitcoin community has chosen the former. If the proposal for protocol using quantity adjustments, rather than difficulty adjustments, is adopted, then that will represent a choice for the latter. Given the dire prospects for the future with climate change, this change should be implemented as soon as possible.

5 Preventing 51% attacks?

Given that it will not be very computationally inexpensive to mine under this alternative framework, one might worry about 51% attacks. This occurs when one miner can mine more than 51% of the blocks, which would allow them to fraudulently add incorrect transactions to the blockchain and enrich themselves, while destroying trust in the blockchain. I do not see that these would be more of an issue under the price-based protocol relative to the status quo. With inexpensive mining, it would also be very cheap for new entrants to mine, even with their smartphones, and have a good chance of being successful, which is not possible today given the difficulty of Bitcoin mining. Nevertheless, this issue is often raised in the context of reducing difficulty, so I will address it anyway. The Herfindahl-Hirschman Index (HHI) measures market concentration by summing the square of the market shares in percent (Rhoades, 1993). We define market shares for the jth miner as s_j as follows:

$$s_j = \frac{M_j}{M} \tag{30}$$

For a given market share, the HHI Index, H, is

$$H = \sum_{j=1}^{N} s_j^2. \tag{31}$$

We can thus make a measure of the concentration for the jth miner, H_j, by taking the jth miner's contribution to the HHI index and dividing by the aggregate index, as follows:

$$S_j = \frac{s_j^2}{H} \tag{32}$$

We define the average share, V, as:

$$V = \frac{1}{N} \sum_{j=1}^{N} S_j \tag{33}$$

We can set up a net transfer, τ, which is defined as:

$$\tau = \alpha_\tau \left(S_j - V \right) \tag{34}$$

α_τ is a nonnegative real number, and will be defined more precisely later. We can show that

$$\sum_{j=1}^{N} \tau = 0$$

because

$$\sum_{j=1}^{N} \tau = \sum_{j=1}^{N} \alpha_\tau \left(S_j - V \right) = \alpha_\tau \left(\sum_{j=1}^{N} S_j - NV \right) = \alpha_\tau \left(\sum_{j=1}^{N} S_j - N \frac{1}{N} \sum_{j=1}^{N} S_j \right) = 0$$

The algorithm would then have a tax and subsidy system of sorts, with a tax imposed on larger players (who are above average) by reducing the amount of new Bitcoin ΔQ they are awarded, which would be used to subsidize smaller players (who are below average), increase their Bitcoin awarded if they are able to hash successfully. The size of the transfer is governed by α_τ, and this should similarly be governed algorithmically based on how close any one player is to the 50% threshold. These could vary, but one potential rule would be

$$\alpha_\tau = 1 - 2\left(\frac{1}{2} - max(s_j)\right) \tag{35}$$

so that as the largest market share goes to zero, the tax goes to zero. When the largest market share is 50%, then $\alpha_\tau = 1$, and this miner will have a large share of the overall HHI Index, so will face a very high tax rate, not far from 100%. This will discourage size and encourage a decentralized mining ecosystem filled with small players. Given that difficulty will be set to 1, the absolute minimum, hashing could occur even on mobile phone or even running in the background on computers. This would allow a broadened participation in the Bitcoin ecosystem relative to the current system. There may be some complains about this concentration tax by larger players, but it should benefit the smaller miners as well as reducing the chance of a catastrophic 51% attack, so should be preferred overall.

6 Conclusion

Bitcoin mining currently consumes an enormous amount of energy. In the summer of 2022, Bitcoin's electricity usage exceeded that of the entire nation of Argentina.[5] However, it does not have to be that way. Bitcoin, like other crytocurrencies based on Proof-of-work, increases the difficulty of the cryptographic problems involved in mining when too much computing power devoted to mining, forcing additional electricity usage, and thus additional carbon emission, unnecessarily. This paper has outlined an alternative, which would instead adjust the quantity of Bitcoin outstanding, and thus the reward ot mining Bitcoin, to discourage mining, while setting the difficulty of mining, and thus the electricity usage involved in mining, to

[5] Source: https://news.climate.columbia.edu/2022/05/04/cryptocurrency-energy/, accessed June 9th, 2022.

the technological minimum. The electricity usage for each framework was derived from a microeconomic model of Bitcoin miners maximizing profits. This would reduce electricity usage by a factor of trillions, bringing the electricity usage down to trivial level, and eliminating environmental concerns about Bitcoin and other cryptocurrencies based on Proof-of-work. This would allow the security benefits of Proof-of-Work without any of the environmental costs.

There are tradeoffs involved with this change, as increasing interest in Bitcoin under this alternative framework would tend to cause capital losses for Bitcoin holders, but an additional advantage is that Bitcoin's potential as a revolutionary, transformative technology, would be able to be fully realized under this alternative. The potential for 51% attacks that could take over the Bitcoin network should not be more of a concern under this alternative framework than under the current set-up, but even so, a tax and transfer scheme is outlined to assuage these concerns.

Cryptocurrencies, and especially Bitcoin, are here to stay. With the ongoing climate crisis, we need to provide a way to address the environmental consequences of cryptocurrencies. While Proof-of-Stake provides an environmentally friendly alternative to Proof-of-Work, there are advantages to cryptocurrencies using Proof-of-Work. All cryptocurrencies using Proof-of-Work should immediately switch to the alternative mechanism outlined in this paper. This would, most importantly, eliminate the excessive environmental costs to Bitcoin mining, but would also broaden access to Bitcoin so that cryptocurrencies can realize their full potential.

References

Baur, Dirk G and Thomas Dimpfl, "The volatility of Bitcoin and its role as a medium of exchange and a store of value," *Empirical Economics*, 2021, *61* (5), 2663–2683.

_ , Kihoon Hong, and Adrian D Lee, "Bitcoin: Medium of exchange or speculative assets?," *Journal of International Financial Markets, Institutions and Money*, 2018, *54*, 177–189.

Briere, Marie, Kim Oosterlinck, and Ariane Szafarz, "Virtual currency, tangible return: Portfolio diversification with bitcoin," *Journal of Asset Management*, 2015, *16* (6), 365–373.

Cain, Mary B and Fernando L Alvarado, "Implications of cost and bid format on electricity market studies: linear versus quadratic costs," in "2004 Large Engineering Systems Conference on Power Engineering (IEEE Cat. No. 04EX819)" IEEE 2004, pp. 2–6.

Cocco, Luisanna and Michele Marchesi, "Modeling and Simulation of the Economics of Mining in the Bitcoin Market," *PloS one*, 2016, *11* (10), e0164603.

Dwyer, Gerald P, "The economics of Bitcoin and similar private digital currencies," *Journal of financial stability*, 2015, *17*, 81–91.

Fetz, Aurelio and Massimo Filippini, "Economies of vertical integration in the Swiss electricity sector," *Energy economics*, 2010, *32* (6), 1325–1330.

Jara-Dıaz, Sergio, Francisco Javier Ramos-Real, and Eduardo Martınez-Budrıa, "Economies of integration in the Spanish electricity industry using a multistage cost function," *Energy Economics*, 2004, *26* (6), 995–1013.

Kraft, Daniel, "Difficulty control for blockchain-based consensus systems," *Peer-to-peer Networking and Applications*, 2016, *9* (2), 397–413.

Martínez-Budría, Eduardo, Sergio Jara-Díaz, and Francisco J Ramos-Real, "Adapting productivity theory to the quadratic cost function. An application to the Spanish electric sector," *Journal of Productivity Analysis*, 2003, *20* (2), 213–229.

Mattke, Jens, Christian Maier, Lea Reis, and Tim Weitzel, "Bitcoin investment: a mixed methods study of investment motivations," *European Journal of Information Systems*, 2021, *30* (3), 261–285.

Podhorsky, Andrea, "What's the Difficulty? Understanding and Incentivizing Bitcoin's Difficulty Adjustment Mechanism," *Understanding and Incentivizing Bitcoin's Difficulty Adjustment Mechanism (April 22, 2021)*, 2021.

Prat, Julien and Benjamin Walter, "An equilibrium model of the market for bitcoin mining," *Journal of Political Economy*, 2021, *129* (8), 2415–2452.

Qiu, Zhifeng, Geert Deconinck, and Ronnie Belmans, "A literature survey of optimal power flow problems in the electricity market context," in "2009 IEEE/PES Power Systems Conference and Exposition" IEEE 2009, pp. 1–6.

Rhoades, Stephen A, "The herfindahl-hirschman index," *Fed. Res. Bull.*, 1993, *79*, 188.

Saleh, Fahad, "Blockchain without waste: Proof-of-stake," *The Review of financial studies*, 2021, *34* (3), 1156–1190.

Schilling, Linda and Harald Uhlig, "Some simple bitcoin economics," *Journal of Monetary Economics*, 2019, *106*, 16–26.

Sharma, Gagan Deep, Mansi Jain, Mandeep Mahendru, Sanchita Bansal, and Gajendra Kumar, "Emergence of Bitcoin as an Investment Alternative: A Systematic Review and Research Agenda.," *International Journal of Business & Information*, 2019, *14* (1).

Velde, Francois R., "Bitcoin: a primer," *Chicago Fed Letter*, 2013, (12).

Vranken, Harald, "Sustainability of bitcoin and blockchains," *Current opinion in environmental sustainability*, 2017, *28*, 1–9.

Yermack, David, "Is Bitcoin a real currency? An economic appraisal," in "Handbook of digital currency," Elsevier, 2015, pp. 31–43.