Metropolitan State College

ICS-690, Spring 2022

Nicholas Connel

White Paper Submission

**Proof of Work**

**Comparisons, Problems, Energy considerations, and solutions**

**TABLE OF CONTENTS**

[**Section 1. What a viable blockchain must do and should do**](#_fasa93eo8eg6) **4**

[**Section 2. Comparison of POW and POS**](#_vqw4btayo58v) **5**

[A. Security](#_lcp8bnop5uoz) 5

[B. Throughput](#_plo9soegpa5u) 6

[C. Efficiency](#_7vnpoudt4m6o) 6

[D. Comparison Recap](#_xhm043il3ewv) 7

[**Section 3: Critics of POW**](#_o209z6y61pxf) **8**

[A. Energy waste, Unsustainability](#_90gc3q3ivx4h) 8

[B. Throughput is inadequate](#_rx04ji1eacej) 11

[C. Vulnerability to the 51% Attack](#_jbfuk37exc4n) 12

[**Section 4. Working with POW, Energy Issues**](#_c9wf9nb8vj6s) **14**

[A. Active Energy Reserve Encourages Renewables](#_v7k5gagxvm1p) 14

[B. Heat Recovery, Case Study](#_f7adabd8n25t) 15

[**Section 5. Conclusion**](#_bsmwpzbhi4r9) **18**

[**REFERENCES**](#_h0enaz4ncjdo) **19**

ABSTRACT

Since the introduction of cryptocurrency in 2009, the types of currencies (coins) have proliferated and the industry market cap has grown to be valued at muli-trillions of dollars. Along with this explosive growth, problems have become apparent as to the scalability of the blockchain architecture that was originally adopted for the first cryptocurrency, Bitcoin.

This paper will examine the distributed consensus protocols, focusing on looming problems that may threaten the health of the cryptocurrency space.

These considerations will lead to proposals to take advantage of trends in the US electric energy sector to help secure the integrity of the cryptocurrency market and synergistically help with the global transition to renewable sources of energy.

INTRODUCTION

With the market cap of the cryptocurrency market at 2.35 - 2.9 Trillion dollars, it is comparable in size to the world automotive industry. Along with such high valuation comes a great deal of interest, activity, and integrity challenges from self interested bad actors.

Since 2009, the main mechanism to accurately maintain the cryptocurrency ledger has been the Proof of Work protocol (POW). POW enables the blockchain network to operate in a decentralized manner and has been in flawless operation since 2009 on the Bitcoin blockchain.

Although there is a great deal of confidence in POW owing to its track record over time, there are valid criticisms and concerns:

* Resource inefficiencies, both computing and energy utilization
* Poor (inadequate) Transaction Throughput
* Theoretical vulnerability to someone controlling over 50% of network

In this paper, each of these points will be examined in detail, along with some comparisons with a newer protocol known as Proof Of Stake (POS).

POS, which has demonstrated several advantages over POW, may eventually become the standard protocol over time. However, due to its much shorter track record, it does not currently enjoy the confidence of POW. Furthermore, the largest crypto by market cap, Bitcoin (BTC), is utilizing POW and has no plans to change currently. For these and other reasons (to also be elaborated on), in this paper it is assumed that POW will be the de facto consensus protocol going forward.

Given the momentum and pervasiveness of POW, consideration on how to enable it to overcome its energy intensity problem will be examined by way of two proposals to develop. The first is to exploit the intermittent nature of renewable energy that is gaining a larger share of the energy sourced for the electrical grid. The second is to capture heat energy that mining computers generate during operation to offset energy inputs in heating applications.

# 

# Section 1. What a viable blockchain must do and should do

For a blockchain backed cryptocurrency to be viable, there are three properties that it must have. These are:

1. Achieve consensus

2. Be secure/immutable

3. Scale up to the intended use case

In addition to these properties, there are 2 others that important and differentiate the POW and POS protocols:

1. Efficient (Both computing and energy utilization)

2. Achieve high transaction throughput

It is assumed here that if a system is both efficient and has a high transaction throughput that it will also be cost effective. In Table 1 below, POW and POS are compared for each of the traits listed above. While POW has a check for each of the “Must Have” properties, it fails at the desired properties. On the other hand, POS has all of the properties with the possible exception of the “Must Have” of security. In the next section, we will take a closer look at these differences.

Table 1: Merit for POW and POS

|  | Consensus | Secure | Scales | Efficient | Throughput |
| --- | --- | --- | --- | --- | --- |
| POW | X | X | X |  |  |
| POS | X | ? | X | X | X |

? Mostly untested; The most history being on Cardono since 2017

# Section 2. Comparison of POW and POS

As can be seen in Table 1, POW and POS differ in Security, Efficiency, and Transaction Throughput. In this section we will take a closer look at each.

## A. Security

POW, for the example of the Bitcoin (BTC) blockchain, has been in continuous operation since 2009. Aside from the inherent 51% attack, it is considered computationally secure. On BTC, POW has suffered no known successful attacks. This despite the BTC market cap to be over 755 Billion dollars (See Table 2). Given this successful track record, POW enjoys great security confidence in the cryptocurrency community.

Table 2: Top 11 Cryptocurrencies; Market Cap and Consensus Protocol Information



POS has been in operation on the Cardano (ADA) network since 2017, and has been followed more recently by several other cryptocurrencies. Like BTC, it has not suffered any major security breaches, although it has neither been around for as long as BTC, nor have nearly the market cap at 31 Billion dollars. There have been critics who point to several potential problems. POS has not had the same level of research done on it as the original POW protocol so there could be theoretical problems. Furthermore, attacks have been devised such as “Nothing at stake”, and transaction censorship have been put forward as potential problems. Protocol designers have tweaked POS whenever a new attack is devised, but it does not have the same time in production as POW, and does not enjoy the same level of confidence in its security.

## B. Throughput

POW has a generally poor transaction throughput. If we look at table 2 for example, we can see the worst performer is BTC, at 7 TX/s. This is built into the protocol as the number of blocks, and bytes per block are time and size limited. Increasing the throughput can be tweaked by altering the block size or frequency, but these changes cannot produce substantial increases and can only moderately increase the throughput. There ways to increase the overall throughput via other means. These will be addressed in the next section.

POS was primarily designed to fix the issue with POW throughput and eliminate the duplication of effort that makes POW a resource hog. Here we will look at throughput, and in the next subsection we will address efficiency.

There is no question that POS has a great theoretical advantage in regard to transaction throughput. The work/competition in POW is eliminated, replaced by actual voting by stakeholders to validate blocks. However, the simplicity is misleading. Many additions to this protocol were needed to address attacks that were discovered. The longest running version of POS, Cardano (ADA), has a better throughput at about 250 TX/s, but this does not blow away what the legacy POW blockchains achieve. Note that this may be limited by the particular implementation. Another more recent example is Avalanche (AVAX) with a throughput of about 4500 TX/s. The proposed Ethereum (ETH) 2.0 hard fork, which among other upgrades, switches from POW to POS, predicts a throughput even higher than AVAX.

## C. Efficiency

The most often heard criticism of POW is the amount of resources that are used in its implementation, and especially the electrical power used by the miners. [1] On the face of it, the question about energy use is a fair one. According to the Cambridge Center for Alternative Finance (CCAF), Bitcoin currently consumes around 110 Terawatt Hours per year — 0.55% of global electricity production. The consequences for global warming due to associated carbon emissions from this generated power seems alarming. Furthermore, this electric load has grown to this level from nothing since 2009. Will this load continue to increase with explosive growth? These questions will be addressed in the following section. For now we will acknowledge that this is indeed a large amount of power, and that POW gets a poor mark for efficiency.

The POS protocol, as mentioned in the context of transaction throughput, does away with the duplication of effort that is at the heart of POW. By eliminating the competition component to arrive at consensus, virtually all of the computational power can be eliminated from your mining network. This makes POS comparable to centralized systems in regard to computational capacity required. It also eliminates specialized equipment that has become prevalent with POW mining operations. For these reasons, POS gets a gold start for efficiency.

## D. Comparison Recap

In every category, POS looks to be the better choice of consensus protocol with the possible exception of security. POS does have some track record in this respect, and indications are good that the protocol is indeed secure. However, as with adopting anything new, some risk is taken. It may be that in the future, POS or some other even better consensus protocol becomes the standard, but the current situation does not indicate that POW is going away. While ETH plans to switch from POW to a version of POS, this is somewhat of a great experiment. This has not been done before, and it is still possible that the change will be aborted because something that as of now is unforeseen.

What's more, referring to Table 2, we can see that the market cap of BTC is greater than that of the next 10 largest cryptocurrencies put together. Since BTC has no plans to switch to another protocol, we can extrapolate that POW will be around for the foreseeable future.

# Section 3: Critics of POW

Although POW is not ideal, it is what most cryptocurrencies are using for a

consensus protocol today and for the foreseeable future. POW has its detractors and they have valid points. In this section we will try to address the most problematic issues. The next section contains proposals to address some of these.

## A. Energy waste, Unsustainability

As mentioned in section 2, its estimated POW mining uses over half a percent of global electrical energy production, and this has risen from nothing in only 14 years. Critics contend that this is contributing to global warming due to the electricity being generated by burning carbon based fuels such as coal. However, [1]much of the power that is used has been from renewable sources. Estimates for what percentage of POW mining uses renewable energy vary widely. In December 2019, one report suggested that 73% of Bitcoin’s energy consumption was carbon neutral, largely due to the abundance of hydro power in major mining hubs such as Southwest China and Scandinavia. On the other hand, the CCAF estimated in September 2020 that the figure is closer to 39%. But even if the lower number is correct, that’s still almost twice as much as is fed into the U.S. grid, suggesting that looking at energy consumption alone is hardly a reliable method for determining Bitcoin’s carbon emissions.

The dynamic of why such a large percentage of energy used in mining comes from renewable sources can be understood from the perspective of competition. The only input for mining, excluding capital for equipment, is electricity. We can readily assume that mining operations will migrate to the lowest cost electricity. Power generated from renewables tends to be not only intermittent, but have excess capacity to compensate for periods of low production. During periods of above average production, the excess power is useless unless some sort of storage is available. Miners can take advantage of such situations and obtain virtually free electricity.

Similarly, otherwise unused energy can be used for electricity generation. For example heat from the flaring of natural gas at remote oil fields can be used to power a generator. Mining with electricity from this source adds nothing to the current carbon output from the oil field.

The global warming associated with POW mining cannot be ignored, but the actual carbon output is not nearly as bad as critics claim. In the long term, all electricity generation will be carbon neutral, and this effect on the environment will go away.

Next, critics have said that energy use by POW is increasing exponentially, and will soon break the grid. While POW mining has gone up continuously since it began, and it started as an exponential rise, it is no longer so. In the next two charts, we can see the estimated hashes per second performed in BTC mining over time. Both charts show the same information with the difference being that Chart 1 shows both axis linear, and Chart 2 has the y-axis (Number of Hashes per Second) on a logarithmic scale. Looking only at Chart 1, it indeed appears as if we may have an exponential rise in the number of hashes per second over time. But, if we look at the logarithmic version, it is easily seen that the rate of increase is coming down over time. Extrapolating, it looks as if we will be reaching a steady state in just a few more years.

Chart 1: Linear Hashes per Second Used by Bitcoin Miners

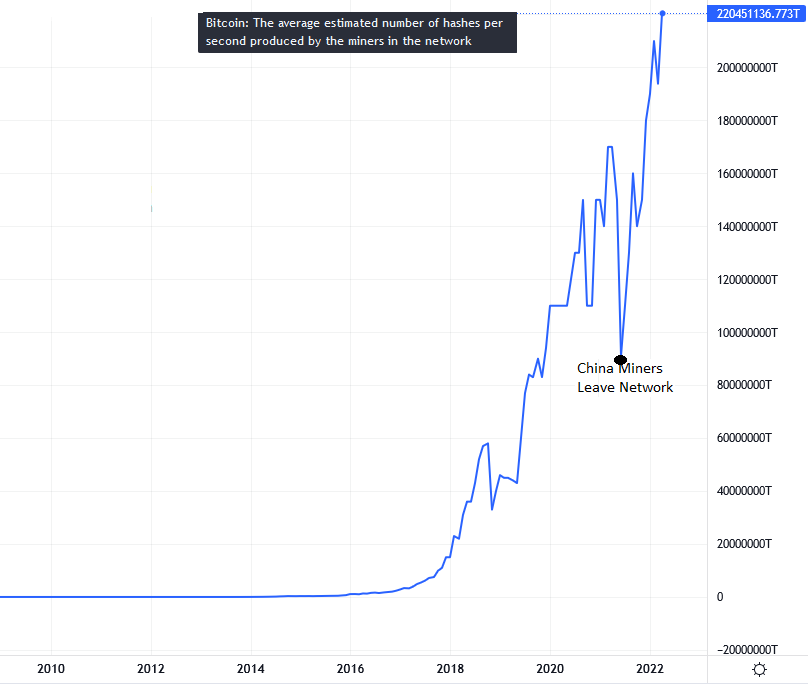
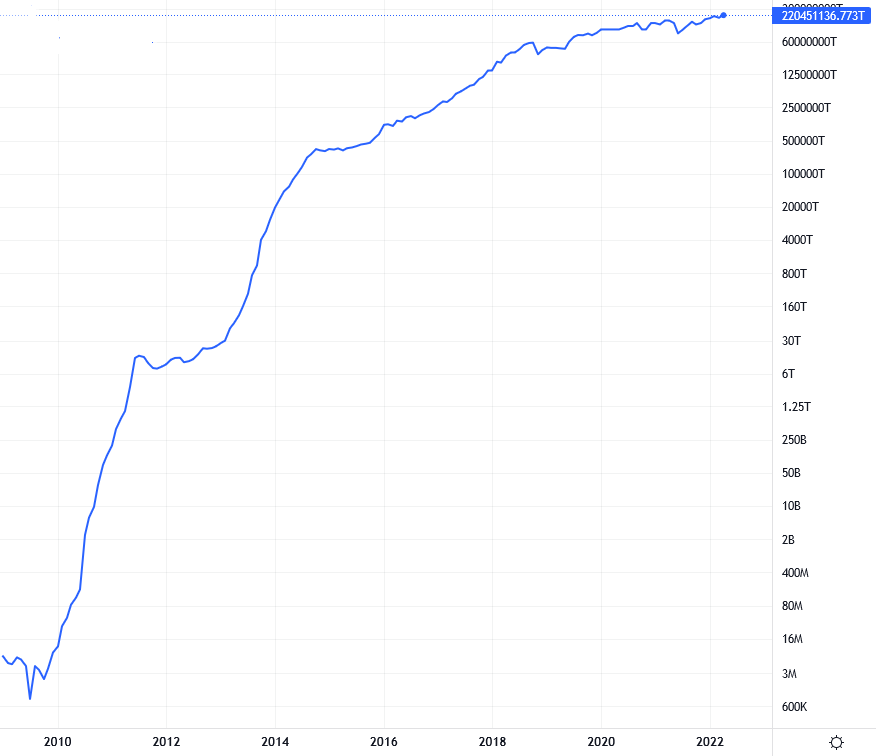


Chart 2: Logarithmic Hashes Per Second used by Bitcoin Miners



Source Charts 1 and 2, Trading View: https://www.tradingview.com/symbols/GLASSNODE-BTC\_HASHRATE/

Furthermore, I predict that the energy used by mining BTC will eventually go into a slow decline after reaching a plateau. This is based on the following factors and assumptions. First factor; BTC block reward will eventually go away. This is designed into BTC and is unlikely to be modified. Approximately every 4 years the per block mined bonus is halved, eventually becoming less then the smallest fractional bitcoin in year 2140. My assumption is that BTC value will become much less volatile over time. As cryptocurrency sees greater adoption in the general economy, volatility should go down as a result. So, in this environment, miners will only make money by servicing transactions on the blockchain. The market size then is tied to the growth in the economy. Natural competition will favor the minors that get the most hashes per watt (the only input for the business), therefore the number of hashes per watt will go down due to inherent innovation.

Overall, the energy use of POW mining is substantial. While it is not unsustainable, neither will it improve to any great extent, even if my future prediction is correct. It is working, but the cost of the power input is a drag on the cost of using crypto. One can assume that when a substantially cheaper protocol (with the risk and transition costs factored in) becomes available, the industry will switch over to it. Until then POW is doing the job.

## B. Throughput is inadequate

POW is built for security not speed. As a matter of fact that is a conscious trade off on the part of the original developers. This is baked into the protocol, and cannot be altered in any substantial way. After BTC, other blockchains were created with their own associated currencies. The first of these all used POW, with various modifications. These new blockchains did improve on the transaction throughput somewhat, but the underlying roadblock was POW itself.

So, to answer the critics of POW claiming that the transaction throughput is inadequate to service a world wide adoption of it for general purpose use, yes that is correct. But is it necessarily the job of the blockchain to handle all of the transactions? Here the answer is a qualified no. Efforts have been made to aggregate ongoing transactions off chain in a second layer and process them on chain when the channels close.

For example, the Lightning Network. The scheme here is to create special funded wallets, called Lightning Wallets, between 2 parties. As more parties create more of these special wallets, each new party can also transact between the parties that the newly connected party is connected to. The transaction is committed to the blockchain when the wallet is closed.

[2]To illustrate, imagine that James opens a channel with his local hardware store and deposits $50 worth of Bitcoin. His transactions with the hardware store can now be facilitated using the Lightning Network instantly.

Heather, who has a different channel open with her local smoothie shop, buys hardware from the same store as James. The connection between James, the grocery store, and Heather makes it possible for James to buy smoothies from the smoothie shop using the Lightning balance he has with the hardware store. Heather can also use her smoothie shop balance to facilitate transactions with other businesses within James’ network.

If Heather were to close her channel with the smoothie shop, then James would have to open a new channel with the smoothie shop to make Lightning purchases there, assuming there are no other available channels open.

[3]The Lightning Network can process hundreds of thousands more transactions per second than the main Bitcoin blockchain, and Fees on the Lightning Network are typically a fraction of a cent. If this system, or one like it, were adopted, the issue with POW’s transaction throughput could be handled.

## C. Vulnerability to the 51% Attack

While POW has been shown to be secure, it is known that if a single actor manages to secure over 50% (a common shorthand for this is 51%) of the mining capacity, they can control the blockchain. Smaller networks, Ethereum Classic (ETC) for example, have fallen prey to this attack, so it should never be assumed that any POW network is immune.

Even BTC, as large as it is, has had a situation where a mining pool hash share exceeded 50% causing a blockchain existential crisis. [4]GHash.IO pool reached 51% control of the Bitcoin network in 2014 for a period of about 12 hours. When the hashpower of the GHash.IOpool reached this high level, the Bitcoin community encouraged each other to leave the pool to prevent the possibility of 51% attacks. The proportion of hashpower in the pool declined dramatically, shutting down towards the end of 2016.

We don’t know if GHash constituted a threat, but when custody of the hashrate is greatly centralized, such organizations become high priority targets for hackers (who under these conditions can be assumed to be bad actors).

The reassuring part of the story is that to resolve the issue the community, by encouraging decentralization, reacted in such a way to preserve the network. This makes sense because the miners, who have a vested interest in cryptocurrency’s success in both equipment and expertise, acted out of self interest to protect their investment.

More recently, there was a great deal of concern over the concentration of hashing power geographically located in China. Driven by very low rates on electric power, huge mining operations began rapidly opening in China and by about 2016, 75% of the world's hashing power was controlled by 5 mining pools located there. The highly centralized Chinese government, it was feared, could use its influence over its citizens to either attempt to profit from controlling the networks, or attempt to destroy the blockchains considering the decentralized systems as a threat. The controversy ended with the Chinese government forcibly shutting blockchain mining operations down and making all cryptocurrencies illegal in July 2021.

Summing up, the 51% attack is truly a problem, economy of scale makes large pool sizes attractive. There is a mechanism that acts as a break to consolidation however. The miners' self interest to preserve their investments in the network acts as powerful negative feedback. This feedback is not always sufficient to halt mining consolidations to avoid attacks as is demonstrated by the 51% attack having been successfully executed on smaller networks. While a cabal buying and renting hashing power to attain 51% may be possible on small networks, it is really infeasible on larger networks. If an attack on BTC were to happen (or another large crypto that uses POW), it would be because of large mining pools either going rogue or being compromised in a high consolidation environment. It is really up to the miners themselves to avoid this by spreading the hashing power around either by running their own node or joining smaller mining pools.

## 

# Section 4. Working with POW, Energy Issues

While POW does have issues with transaction throughput, and is sensitive to mining consolidation, the number one issue that critics have with POW is its carbon footprint implied by its considerable energy input. The European Union (EU) has even been considering banning POW mining for this reason. In this section we examine possible ways to mitigate these concerns.

## A. Active Energy Reserve Encourages Renewables

With the coming deep penetration of renewable sources onto the electrical power grid a fundamental change is required. While the legacy system was designed to produce power to match a changing and fairly random load, the renewable based system will seek to match the load to a changing and fairly random power production. The design questions are:

1. How do I meet the peak demand

Like the old system, the new system could fire up a natural gas peaker plant, but this is of course non-renewable. If we are going to stick to our guns, we either have to have stored power (batteries for example), or rely on having over-built capacity to meet the highest demand. Either of these solutions work, but the expense differential may be substantial. At the current price of battery storage at grid scale, it is cheaper to overbuild capacity.

1. What do I do with all the extra power when demand is low

Here is where POW mining can be useful. In our system electric power cannot be stored (no batteries). Therefore a high intermittent (can be turned on or off easily and fairly quickly) load is called for. As crypto mining generates revenue, adopting this scheme makes renewable sourced power more economical, i.e. encourages adoption; a very good thing. Below is an example of such a system that is in Sweden:

“[5]Around 15,000 cryptocurrency mining rigs are humming away at HIVE Blockchain’s (HIVE) 30 megawatt (MW) data center in Boden, Sweden. But not all the time. Sometimes, the facility powers down to help the local grid.

The data center, drawing cheap energy from local hydropower producers, acts as one of the largest, if not the largest, active energy reserves the Swedish grid can call upon whenever there are major disturbances to the local power supply. The facility can shut down its machines almost instantaneously so that energy can quickly be diverted to public use.

“In five seconds, we have to power down half of what we have allowed into the system,” said Johanna Thornblad, HIVE Blockchain’s Sweden country president. “And within 30 seconds, the entire power supply that is being requested has to be participating in the FCR-D system” – the Frequency Containment Reserve for Disturbances that keeps the lights on in the region.

When managed like that, the energy demand of HIVE’s mine is an asset to the local electricity grid; the miners are a stable source of cash flow when public energy consumption is low, but can power off during peak hours.”

IMHO, this type of system would work even better for wind power generation. The wind is a lot more variable, and if the renewable source is hydro, a certain amount of this energy can be stored by allowing the water level in the reservoirs to rise during periods of low demand.

Electrical energy storage, be it in batteries or reservoir levels or something else, is also being integrated into the modern grid. The grid network will incorporate both active loads and energy storage in whatever configuration is most cost effective. The case for mining is greatly enhanced by the revenue it generates and may well help us to design the carbon free grid of the future.

## B. Heat Recovery, Case Study

Whenever an electric current runs through a load, it generates heat. If you need heat, it does not matter if you run the current through a load or an electrical heater[[1]](#footnote-0), you will get the same amount of heat. Using this principle in the case of home heating, the following is a case study utilizing the heat generated by the model crypto mining operation to offset the heat needed to heat the home. One assumption is that all homes will eventually be switching some form of electric heat as we move towards a carbon neutral energy model.

The scenario is a home needs to purchase a new heating system. The choices are a geothermal heat pump, or resistance heating with a mining rig providing some of the heat. The term of the study is 6 years. This amount of time was selected to match the typical lifespan of similar mining equipment. The model accounts for financing costs and equipment costs on a monthly payment system. The savings derived is:

[The amount than what would have been paid for amortized heat pump over 6 years + Cost of electricity used by the heat pump over 6 years]

-

[The amount that you paid for Resistance Heat for 6 years - Income from mining].

The result is a cost savings of $9064.50 over the course of the 6 years.

## 

NOTES:

* The heating equipment for resistance is set at zero. This type of equipment costs much less than a geothermal system, but obviously more than nothing. Increasing this value skews the result more favorably towards the heat pump scenario.
* The full equipment cost of the mining rig is paid over the course of the study, and the value after 6years is not included anywhere (as if it were zero). Adding a value for this skews the result more favorably towards the crypto mining system.
* The cost of electricity @ $0.10/KWh is estimated.
* The S19J Pro BTC mining rig cost is from Amazon. If I had shopped this out I probably could have found a better price.
* Since the Geothermal Heat Pump can also perform as an air conditioner, that system cost was credited $6000.
* The revenue figure of 0.2 $/Day/(TH/s) was for April 14th, it is variable but this is a good estimate on the low side of historical averages.

Note that the mining rig is sized to offset 40% of the heat required for the home. Increasing the relative size of the rig would increase the revenu, and the monetary savings.

This is a simple example of heat recovery. There is no reason that this system can not be used to also be an active load as described in 4A, albeit a small one.

# 

# Section 5. Conclusion

Proof of Work has been the workhorse protocol of blockchain technology. While it has problems and there are other protocols with improved specs such as POS in contention, momentum and risk avoidance may well keep this protocol as the prime consensus mechanism for some time to come. The main problems with POW; Poor transaction throughput, its vulnerability to mining consolidation, and energy intensiveness, are inherent qualities and cannot be changed in significant ways without fundamentally reengineering the protocol.

If throughput is going to be addressed, POW will require some type of off chain solution. Be it the Lightning Network, or something else, it is an active area of investigation.

The consolidation problem can only be handled off chain as well. The community needs to self police in order to avoid high levels of pool consolidation and be watchful of hashing power getting too centralized.

The oversized energy use is non-ideal, but it is something that can be handled. The exponential growth phase of the electrical power input is in the past. Going forward, the problem can be mitigated by using “waste” heat in such a way as to eliminate the mining energy footprint. Also, we can turn around the carbon footprint issue by making mining a beneficial active load on the electric grid of the future.

# 

# REFERENCES

[1] Nic Carter, “How Much Energy Does Bitcoin Actually Consume”, Harvard Business review, May 2021

[2] Brian Nibley, “What is the Bitcoin Lightning Network? How Does it Work?”, SoFi Learn; <https://www.sofi.com/learn/content/lightning-network/>, July 2021

[3] BitPay; <https://bitpay.com/blog/bitpay-supports-lightning-network-payments/>

[4] Stefania Stimolo, “The Rush for the Hashpower”, Nova Mining; <https://medium.com/novamining/the-rush-for-the-hashpower-408f642cac6a>, Jan 2018

[5]E. Gkristi, S. Handagama, “Can Crypto Miners Make the World Greener?”, CoinDesk, <https://www.coindesk.com/layer2/miningweek/2022/03/26/can-crypto-miners-make-the-world-greener/>, March 2022

1. This is true for resistance heat. A heat pump is more efficient. [↑](#footnote-ref-0)