Department of Mechanical and Aerospace Engineering

An Analysis of Bitcoin and the Proof of Work Protocols Energy Consumption, Growth, Impact and Sustainability

Author: David Taylor

Supervisor: Professor Joe Clarke

A thesis submitted in partial fulfilment for the requirement of the degree
Master of Science
Sustainable Engineering: Renewable Energy Systems and the Environment
2018

Copyright Declaration

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree.

Signed: D.Taylor Date: 24/08/2018

Acknowledgements:

I wish to thank Professor Joe Clarke for his guidance and advice through out this project.

I would also like to thank Zsuzsanna, Ali and Emma for their tireless support over the past year and throughout my studies.

List of Figures

List of Tables

1 Abstract:

This report analyses the electrical demand of the Proof of Work Consensus mechanism and the Bitcoin network, its impact on the global electrical supply and its sustainability from an energy perspective. Current and future electrical demand estimations have been achieved through the development of an energy estimations tool, and the analysis of mining hardware trends. Further work was undertaken to analyse historic and future growth and compare the efficiency of this network to current financial infrastructure. The results indicated that despite a decline in value, the network and its energy demand are expanding exponentially. Historic analysis shows that during previous mining phases the network electrical demand was far greater, while future estimates highlight the unsustainable growth rates of the eco system that we are currently witnessing. Comparison of the legacy-banking infrastructure suggests that while Bitcoin is far less efficient as an individual transaction layer, when current payment processing layers are combined the efficiency difference is reduced considerably. The findings suggest that historic growth rates are unsustainable in terms of current electrical supply, and further growth will likely focus on utilising low LCOE, dispatchable Renewables in order to reduce operating costs. Should Bitcoin or any PoW based cryptocurrency become a dominant digital payment method; continued growth in mining operations will require considerable new deployment in order to reduce the resulting pressure placed on current generation infrastructure. Coordination between mining operations and energy producers to reduce curtailment of generation assets and increase profitability is one possible applications of this emerging industry. Due to the lack of central governance and decentralised nature of this technology should price rise without technological progress in mining hardware, it is inevitable the electrical demand of the network will continue to rise over time. National Energy policy makers must start to focus on the connotations and understand the impact on electrical networks of this emerging industry, consider the negative and positive implications and develop policy that accepts this industry but protects energy markets and consumers.

2 Introduction

It is well known that our ‘Financial infrastructure is currently a mess of closed systems. Gaps between these systems mean that transaction costs are high [Provost 2013][1] and money moves slowly across political and geographic boundaries [Banning-Lover 2015; CGAP 2008][2][3]. This friction has curtailed the growth of financial services, leaving billions of people underserved financially [Demirguc-Kunt et al. 2015][4]. To solve these problems, we need financial infrastructure that supports the kind of organic growth and innovation we’ve seen from the Internet, yet still ensures the integrity of financial transactions.’ ‘We trust established financial institutions and do our best to regulate them. But this exclusivity conflicts with the goal of organic growth. We need a worldwide financial network open to anyone. The challenge for such a network is ensuring participants record transactions correctly. With worldwide reach, providers won’t all trust a single entity to operate the network. A compelling alternative is a decentralized system in which participants together ensure integrity by agreeing on the validity of one another’s transactions. Such agreement hinges on a mechanism for worldwide consensus’ (David Mazieres, Stellar Lumen, 2015)[5].

It is easy to highlight the flaws and challenges of the legacy banking system with grandiose proposals, but the solutions put forward regularly fail to reveal the implications of these proposed resolutions. Combined with regular sensationalist reporting; the sustainability, scalability and ultimately the viability of these proposed solutions must be clarified in order to ensure the correct path is taken by decision and policy makers.

Figure 4 Public Interest in Blockchain, Source: https://www.hiringlab.org/2018/03/28/blockchain-job-searches-remain-high/

There is little doubt that the current financial system is in the process of digitalisation be it at the core infrastructure layer or consumer habits. Ensuring the proposed improvements to this system do not have a negative impact is essential. 2017 saw a 14% rise in UK debit card payments over taking cash to become the dominant payment method in the UK for the first time.[6] This coincided with an all-time price high for Bitcoin the dominant cryptography based digital currency, and an unprecedented rise in public interest of block chain technology, crypto currency and their potential impact on the legacy banking system. Many advocates of this technology tout Bitcoin and Blockchain to succeed the global banking network but fail to address the possible implications and challenges still to be overcame such as the energy intensity or transaction speeds. With this said recent disruption to the European Visa payment system highlight the vulnerability, public dependency and necessity for a digital payment system to remain secure and uninterrupted, something that Bitcoin and the Proof of Work Consensus mechanism has so far achieved.[7]

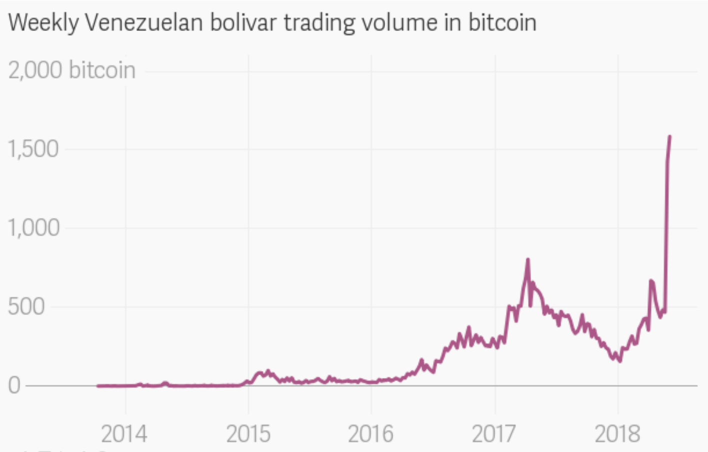


Figure 5 Venezuelan Bitcoin Trading, Source: https://www.theatlas.com/charts/BJhNSW_gm

Venezuela has experienced hyperinflation in recent years and as a result, we have witnessed a 13860% rise in inflation with the IMF suggesting this figure could reach 1 million % by years end should a remedy not be found.[8] We have subsequently seen the nation turn to cryptography, the creation of their own national cryptocurrency (Petro) and in recent months a surge in the use of Bitcoin within their borders as both government and populous look to circumnavigate the resulting economic and humanitarian crisis. As a state and its people appear the first to look to this emerging industry as a means of fiscal autonomy on a national scale, it is essential that the wider implications such as its sustainability be addressed. As such, this paper intends to identify the true energy demand of the proof of work consensus mechanism and its dominant currency Bitcoin, to estimate the current and future energy implications and to compare the sustainability of this with the legacy banking system.

Like any system, the bitcoin block chain has several positive and negative connotations, often cherry picked by critics and advocates depending on their position then regularly inaccurately quoted and sensationalised by the media. The Bitcoin consensus mechanism PoW is rooted in SHA256, which to this date is yet to be hacked proving the viability of this system thus far from a security perspective. The Decentralization of this system is a key aspect of bitcoins success, but the potential of an unregulated market to become centralised appears largely ignored. To take control of a Blockchain 51% of the total network hash rate is required to undertake a DDOS attack, how this translates to energy is a matter for debate, with some claiming 50% of global electricity generation must be consumed before it is considered truly secure. As this system grows exponentially, this becomes increasingly difficult and costly to realise, suggesting that after a certain level of growth only nation states or large organised entities with exceptional resources have the means to undertake such an attack.

Satoshi Nakamoto assumed that only CPU's would be utilised in the mining process, however as is normal with any resource intensive and competitive process, it quickly became apparent that this has created an economy of scale, where from an individual mining perspective a greater hash rate increases the probability of finding the next block first.[9] This has caused mining equipment to evolve rapidly, for the process to become industrialised and seen the partial centralisation of mining by several large parties, and resulted in an alarming level of electrical consumption raising valid concerns over the sustainability of this network. As we witness global efforts to curtail energy consumption and climate change, does the rapid rise of crypto currencies impede these efforts, and does the promised economic inclusivity and immutability of bitcoin and Blockchain justify the allegedly staggering energy demand of such networks and can current proposals such as PoS or the Lightning Network alleviate any of these concerns?

3 Abbreviations, Key Definitions and Background Knowledge

3.1 Abbreviations:

1. Proof of Work: PoW
2. Bitcoin: BTC
3. Reusable Proof of Work: RPOW
4. Denial of Service: DDoS
5. Proof of Stake: PoS
6. Peer to Peer: P2P
7. Application Specific Integrated Circuit : ASIC
8. Computer Processing Unit : CPU
9. Graphics Processing Unit : GPU
10. Field Programmable Gateway Array: FPGA
11. Transactions : Tx

3.2 Key Definitions and Background Knowledge:

3.2.1 Blockchain:

A P2P ledger system designed to remove the necessity of trust between two parties conducting a transaction in the absence of a central authority. New Transactions are bundled and added in blocks chronologically to the ledger by nodes (miners) in the system. A copy of this ledger is automatically distributed to these nodes (computers in the network) allowing for an indisputable cryptographically time stamped record of transactions.

3.2.2 Hash functions:

Hash functions are any function used to map data of any size and to return a hash value or digest of fixed length, allowing for accelerated look up or identifications of duplicates within a large file. Bitcoin utilises cryptographic hash functions, a mathematical algorithm designed to be a one-way and infeasible to invert. 'In the bitcoin protocol, hash functions are part of the block hashing algorithm which is used to write new transactions into the Blockchain through the mining process.' [10]

3.2.3 Proof of Work:

Proof of Work is an economic based consensus mechanism to ensure network security and integrity. It intentionally resource intensive by design, as it is a piece of data that is difficult to produce (costly, time consuming) but easy to verify. The concept originally proposed by Cynthia Dwork and Moni Naor in 1993[11]. In 1997 Adam Back developed this concept further creating Hashcash PoW function to reduce email spam and Denial of service attacks (DoS).[12] By ensuring a modest amount of computing power was allocated to each email the associated time, energy requirements and ultimately costs become too significant to make attacks viable or worthwhile. In 1999 computer scientist, Hal Finney developed RPOW. Building on this concept, Finney proposed an electronic token money that was guaranteed by the value of the real world resources required to mint a PoW token without having to repeat the energy intensive minting process in future transactions.[13] Like RPOW, It is the Hashcash PoW system that Bitcoin utilises for block generation, with decentralized nodes verifying transactions in the P2P network.

3.2.4 Hash (Rate):

Hash is the output of a hash function; it is a measure of the number of times a hash function can be computed per second. A higher hash rate increases the probability of finding the next block in PoW mining and as such profitability is directly propionate to the hash rate. In the instance of Bitcoin the hash function SHA256 is utilised.

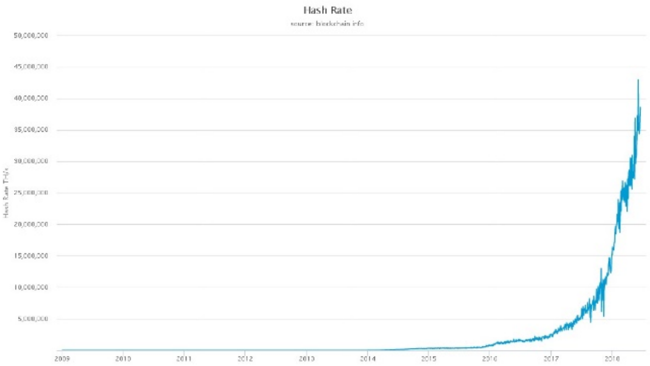


Figure 6 All time Network Growth, Source: https://blockchain.info/charts/hash-rate?timespan=all

3.2.5 SHA256:

SHA256 is rooted in the SHA 2 cryptographic hash function developed by the National Security Agency. It is a mathematical operation run on digital data by comparing the hash output to a known value it can evaluate the integrity of the data and determine if it has been modified or tampered with. It is considered 'collision resistant' meaning no one can find two differing input values that result in the same hash output [14][15]

3.2.6 Mining:

Mining is the process by which new currency is minted and transactions are verified and added to the block chain or public ledger. This involves the compiling of recent transactions and trying to solve a mathematical computational puzzle first. It is a competitive process in which each node or miner repeats the hash function as quickly as possible in order to maximise their probability of finding a valid hash. The miner or node that solves this puzzle first adds the next block to the Blockchain and receives the reward. The reward is the newly minted coins and the transactions fees from the transactions added to the particular block. This reward is the incentive for miners, and the as the probability of solving the computational puzzle is dependent on the hash rate of the equipment solving the puzzle. As this process is resource intensive and a competitive process there is an economic necessity to optimize hash rate and thus use the latest and most efficient equipment available.

3.2.7 ASIC:

ASIC or an Application Specific Integrated Circuit is an integrated circuit designed for a specific use. Previously CPU, GPU and FPGA's were deployed in the mining process, with the original intention stated in Satoshi Nakamoto's White Paper referring to PoW as 'essentially one CPU-one vote'. Within several years miners looking to gain a competitive edge moved to GPU's, then FPGA's in order to optimize their computational hash rate.

3.2.8 Bitcoin Security protocol:

(Prat and Walter, 2018) state that Bitcoin's security model relies on a hybrid approach that combines the robustness of its cryptographic primitives with the economic incentives of the agents participating in the execution of its protocol. In particular, miners play a central role as they stack transactions into blocks and timestamp those in a cryptographically robust way by adding a "proof-of-work". The cost of attacking Bitcoin is proportional to the computing power deployed by miners because it determines the difficulty of the cryptographic puzzles included in the proofs-of-work.[16]

3.2.9 Network Difficulty:

In order to ensure the block time remains constant while the hash rate of mining equipment and the network increase, the network difficulty is introduced as a function of hash rate to regulate the time between blocks. The difficulty is adjusted every 2016 to ensure that a new block is produced roughly every 10 minutes.

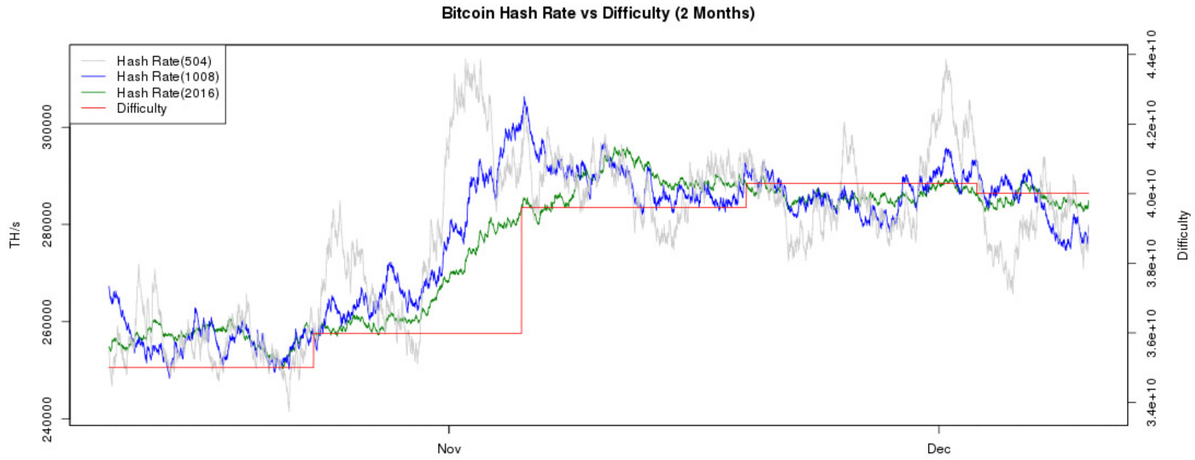


Figure 4 Hash Rate and Difficulty Relationship, Source: https://cryptomining-blog.com/tag/bitcoin-difficulty/

3.2.10 Proof of Stake:

PoS is an alternative to the Proof of Work system that seeks to address the energy intensity of the protocol. Instead of requiring increasing computing power during the mining process, PoS allocates mining to nodes in the network based on the quantity of coins they are holding or their stake and trust is upheld by the stake of the node being utilised as collateral. As a node does not require increasing amount of computing power to remain competitive, the energy intensity of the protocol is reduced.

3.2.11 Lightning Network:

The Lightning Network is proposed solution to increase the transaction volume of the Bitcoin Blockchain. It is a second layer off chain protocol designed to facilitate fast micro transactions. Using a PoS model and nodes within the network, in theory it is intended to resolve the transaction scalability problem facing Bitcoin and other cryptocurrencies.

3.2.12 Block Reward:

The block reward is the reward allocated to miners for the creation of each new block. This reward currently stands at 12.5 BTC per block and halves approximately every 4 years or 210000 blocks, and is due to halve again in May 2020. The block reward halving is an economic measure introduced by Nakamoto comparable to quantitative easing, by reducing the reward scarcity in order to maintain inflation.

4 Literature Review:

Several attempts have been made to estimate the energy demand of the Bitcoin network and its overall sustainability, with the results and methodologies regularly debated, reported and sensationalised. Amongst the most prominent estimations are two stand out works (Alex de Vries, 2018, Marc Bevand, 2017). Both approaches have their individual merits and limitations; the final results produced by each highlight the varying energy demand estimations and the difficulties in reaching consensus on accurate methodologies and results. There are several core challenges facing those interested in modelling and forecasting of the networks energy demand that must be overcame:

- Transparency of ASIC manufacturers and Mining Operations
- Constantly Changing Profitability
- Reliable Data sources
- Varying Regional and Private Electricity Costs
- Mining hardware Progression

4.1 Alex de Vries – Bitcoins Growing Energy Problem[18]

De Vries states that the majority of previous estimations have been made using current hardware efficiencies (J/GH) but highlights the limitations of utilising total network hash rate as the main technique to estimate network power consumption. 'While it is possible to observe the total network hash rate, the devices generating this at each node are implausible to identify without first-hand knowledge of the node, and as mining is a highly competitive and secretive business there is little information regarding which devices are being deployed by these nodes or miners.' Thus while hash rate and the current most efficient devices can produce a best case scenario for network energy consumption, how the total network hash rate is broken down between devices is a challenge in its self.

4.1.1 Economic Based Approach

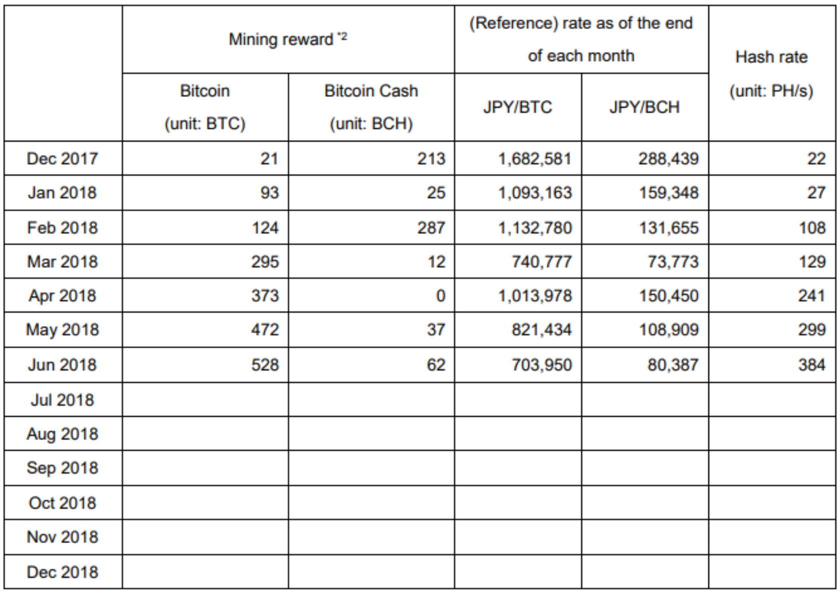
De Vries is critical of a hash rate based approach as it offers no insight into future energy requirements, and instead insists on an economic approach using Adam Hayes[19] work to validate the assumption that 'miners will produce [hash calculations] until their marginal costs equal their marginal product'. Once equilibrium is reached where it is no longer profitable a miner will either stop mining or replace the equipment with more efficient devices. In order to establish an economic approach De Vries builds on Adam Hayes work and takes hardware costs as well as electricity costs into account. By doing so an estimation of hardware costs must be made in order to establish at which point market equilibrium and profitability can be estimated. Again building on work by Jimmy Song[20] and adapting it to the task De Vries has had to make several assumptions in order to estimate production costs, lifespan, and total life cycle costs of the leading hardware the Ant miner S9. While increasing the number of assumptions may reduce the credibility of the work, De Vries has uncovered numerous pieces of critical research, brought it to the forefront and has not shied away from the potential shortcomings of so many assumptions. One potential shortcoming is the assumed global electricity price of $0.05 KWh, BITMAIN have acknowledged they pay less than this per KWh and it is likely that many others, specifically in China pay less than this too, while many small scale miners will likely pay more. Another shortcoming of this approach is the varying sale price of mining hardware, as the retail and resale value of these machines varies with coin price and demand.

4.2 Morgan Stanley, GMO and Bitcoin Miner Production [21][22]

As previously stated ASIC production details are understandably difficult to acquire especially from a privately owned company. After the price of Bitcoin and thus profitability dropped in 2014 many ASIC manufacturing start-ups went in to bankruptcy (as highlighted in Figure 5), this allowed for the surviving manufacturers to take larger shares of the market and in recent years BITMAIN have become the industry leading manufacturer. Centralisation of hardware manufacturing has serious implications for a decentralised network as it allows for the possibility of centralised control of the network. As such it is not in BITMAINS interests to reveal such data but critical from an investment perspective to establish their market dominance. This has led to Morgan Stanley conducting their own investigation into BITMAINs production output of the Antminer S9 whom suggest BITMAIN have a market share of 70%.

This has been achieved through a chip based production estimate and data requests of TSMC (Taiwan Semi-Conductor Manufacturing Company) a publicly listed company who supply the chips for BITMAINs Antminer. Morgan Stanley estimate that ‘with 20000 16nm wafers a month being ordered, each wafer capable of supplying chips for 27-30 mining rigs per month Bitmain could produce half a million Antminer S9 per month.’

Unlike the majority of mining ASIC manufacturers, the Japanese company GMO Internet have submitted the monthly statistics from their mining business with their Quarterly reports. This allows for an indication to the number of rigs produced by the company as the mining equipment is due for release to the public in October 2018. This gives more accuracy to weighted average estimates and allows for better analysis of Morgan Stanley's BITMAIN production estimates. It also highlights the practice of tech companies taking pre sale orders then using the mining equipment during their most profitable period prior to the release of the devices to the public.



	Mining reward *2		(Reference) rate as of the end of each month		Hash rate (unit: PH/s)
	Bitcoin (unit: BTC)	Bitcoin Cash (unit: BCH)	JPY/BTC	JPY/BCH	
Dec 2017	21	213	1,682,581	288,439	22
Jan 2018	93	25	1,093,163	159,348	27
Feb 2018	124	287	1,132,780	131,655	108
Mar 2018	295	12	740,777	73,773	129
Apr 2018	373	0	1,013,978	150,450	241
May 2018	472	37	821,434	108,909	299
Jun 2018	528	62	703,950	80,387	384
Jul 2018					
Aug 2018					
Sep 2018					
Oct 2018					
Nov 2018					
Dec 2018					

Figure 5 GMO Q2 Mining Operation Report, Source: https://ir.gmo.jp/en/pdf/irlibrary/disclose_info20180803_e.pdf

4.3 Marc Bevand- Electricity Consumption of Bitcoin: A Market Based Approach [23]

The approach taken by Marc Bevand offers a more detailed account of the mining ASIC history, as well as how and why many of the assumptions were reached. The analysis offers a detailed insight and breakdown of the methodology, data sources, the economics of mining and the profitability threshold assumption used to estimate total network electricity consumption. Bevand has managed to acquired manufacturing data from one of the leading ASIC manufacturers Canaan, allowing for an increased accuracy in estimating hash rate breakdown. This approach has utilised 3 scenarios to estimate best, worst and most likely case assumptions on mining equipment, where worst case scenario indicates the least efficient but profitable equipment is deployed and best case assumes the entire network is utilizing the most efficient hardware.

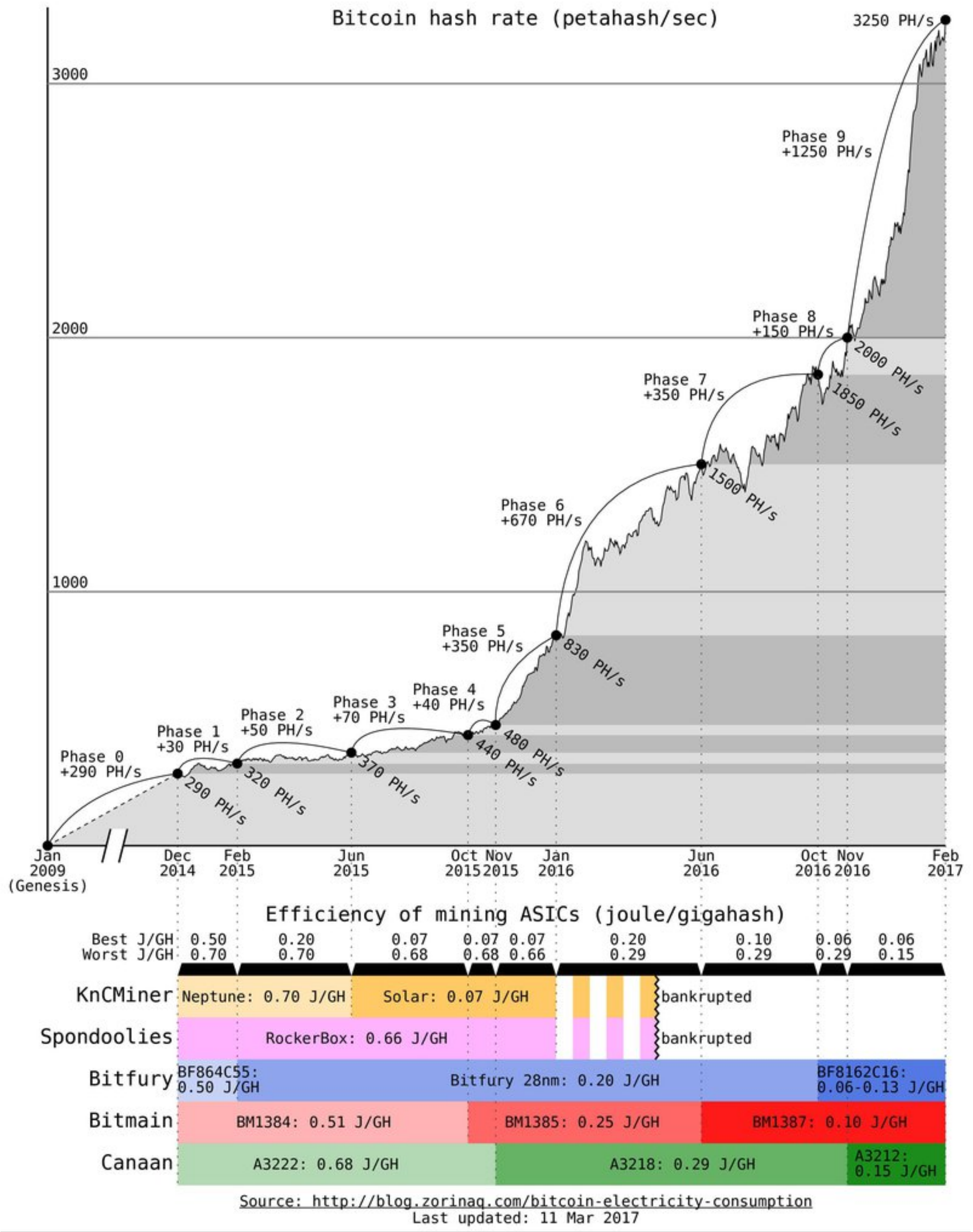


Figure 6 Marc Bevand's ASIC History and Efficiency Chart, Source: http://blog.zorinaq.com/bitcoin-electricity-consumption/#profitability-threshold-assumption

4.3.1 Economics of Mining

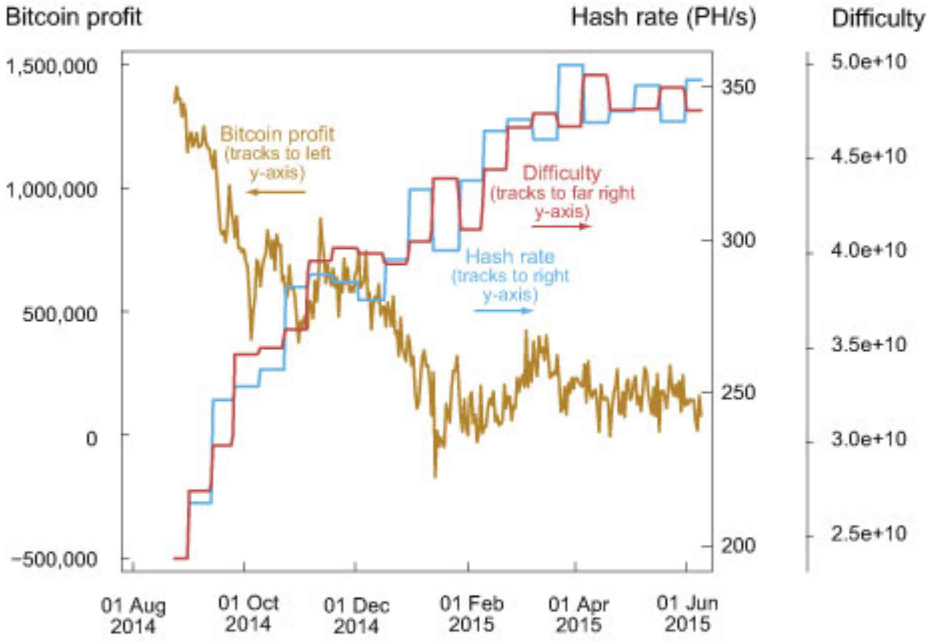


Figure 7 Example of the Profitability/Economics of Mining as Hash Rate and Difficulty Increase, http://libertystreeteconomics.newyorkfed.org/2015/08/entry-and-exit-leads-to-zero-profit-for-bitcoin-miners.html

To demonstrate the economics and profitability of mining, the daily profits and costs of prominent ASIC hardware has been modelled. Figure 6 highlights the necessity for quick deployment of hardware by miners due to the decreasing profitability resulting from increasing hash rate and difficulty. While the majority of hardware modelled by bevand is now unlikely to be profitable, the methodology and assumptions offer a strong basis for further work and future calculations. Analysis of the results produced also highlight the necessity to operate the latest and most efficient hardware with 70% of lifetime profits being generated in the first 30% of the machines life and 80% of profits in the first 50%. Analysis also highlights that with rapid price increases it is possible for hardware that has become unprofitable to become profitable once again and be redeployed, adding further complexity to estimations of how the network is broken down.

4.3.2 Profitability Threshold assumption

Usually only one assumption is used to estimate the profitability of individual mining equipment, the price of electricity. By comparing the efficiency of the best and worst case scenarios with the profitability threshold, Bertrand has managed to validate his methodology. As such, a similar profitability equation will be utilised for these calculations, as it appears to be a good basis for further work. It is unlikely however that the entire network is made of identical hardware and the profitability of each unit with a differing electrical draw must be considered in order to make a more accurate estimation of the network electrical demand. Sourcing accurate data that reduces the assumptions of which hardware make up the network will crucial in establishing more precise network electrical demand estimations.

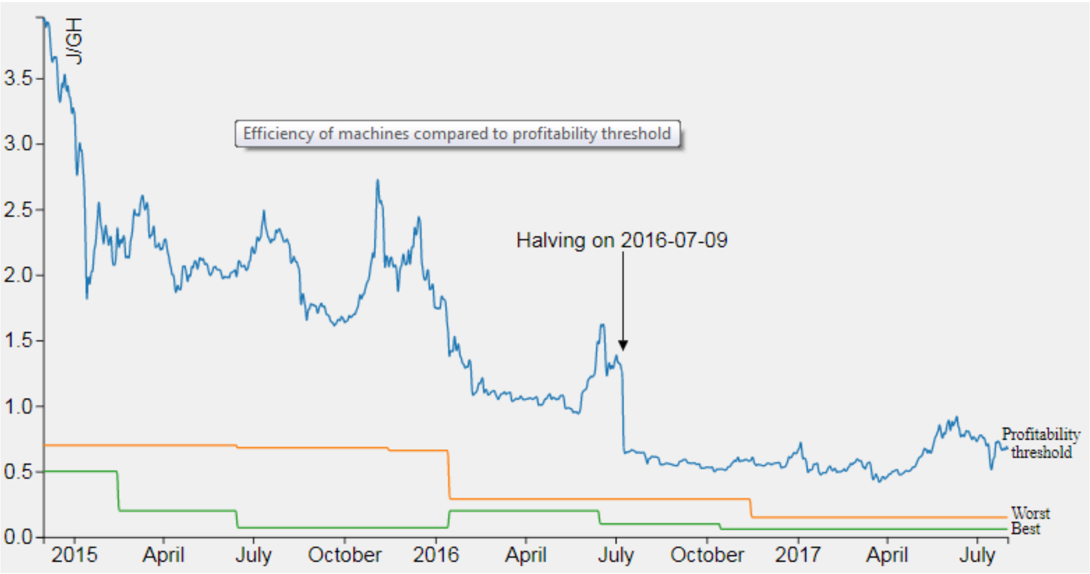
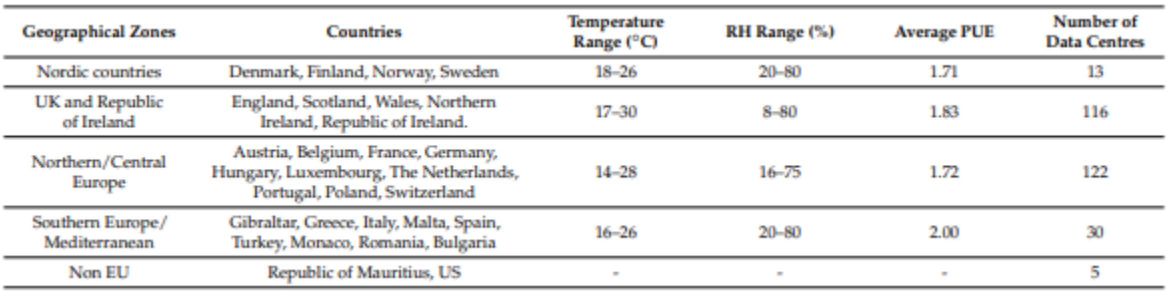


Figure 8 Marc Bevands Profitability Threshold compared leading Hardware Efficiency over time, Source: http://blog.zorinaq.com/bitcoin-electricity-consumption/#profitability-threshold-assumption

4.4 Data Centre Cooling and PUE Considerations

$$\boldsymbol{Power\ Usage\ Effectiveness} = \frac{\boldsymbol{Total\ Facility\ Power}}{\boldsymbol{IT\ Equipment\ Power}}$$

Cooling and additional hidden energy demands are a major consideration of any data centre, and it appears largely overlooked by the majority of estimations due to the difficulty of finding accurate data. This is referred to as the PUE (Power Usage Effectiveness) and De Vries highlights that without this consideration the estimations are limited in their accuracy. As this industry develops, the inefficiencies of data centres are becoming a serious consideration and as such market leaders have begun to optimize mining farm efficiency through relocation and solutions such as immersion cooling, with a claimed PUE of 1.02. De Vries suggests this would account for less than 1% of total network hash rate while Bevand insists that unlike conventional data centres mining operations aggressively optimize their PUE.



Geographical Zones	Countries	Temperature Range (°C)	RH Range (%)	Average PUE	Number of Data Centres
Nordic countries	Denmark, Finland, Norway, Sweden	18–26	20–80	1.71	13
UK and Republic of Ireland	England, Scotland, Wales, Northern Ireland, Republic of Ireland.	17–30	8–80	1.83	116
Northern/Central Europe	Austria, Belgium, France, Germany, Hungary, Luxembourg, The Netherlands, Portugal, Poland, Switzerland	14–28	16–75	1.72	122
Southern Europe/ Mediterranean	Gibraltar, Greece, Italy, Malta, Spain, Turkey, Monaco, Romania, Bulgaria	16–26	20–80	2.00	30
Non EU	Republic of Mauritius, US	-	-	-	5

Figure 9 Geographical Zoning of Data Centre; Typical Temperatures, Humidity and Average PUE, Source: Trends in European Data Centre Energy Consumption (Avgerinou et al 2017)

Investigation conducted by the European Commission into typical data centre PUE within Europe indicates that the PUE estimations of 40% by Morgan Stanley are accurate for conventional data centres, with the current average PUE of 1.6. The report also highlights the advantages in cooling requirements that colder climates such as Nordic countries have and the impact this has on reducing the PUE. Several of the largest mining farms that are publicly known are located in such regions in order to take advantage of the favourable climate. Bitfury have moved to Norway, the Bitmain Oros mine is located in Inner Mongolia and there are several companies situated in Iceland including Bitfury and Genesis Mining. Bitfury have embraced immersion cooling and claim a PUE OF 1.05[24] in their Norwegian 40MW mine, and Bitmain claim a PUE of between 1.11-1.3 for their Oros mine but have not allowed independent verification of these figures while North American GIGA Watt Mining claim to have achieved a PUE of 1.05 using air cooling. The evidence and conflicting information suggest these figures should be approached with caution and scepticism. There are

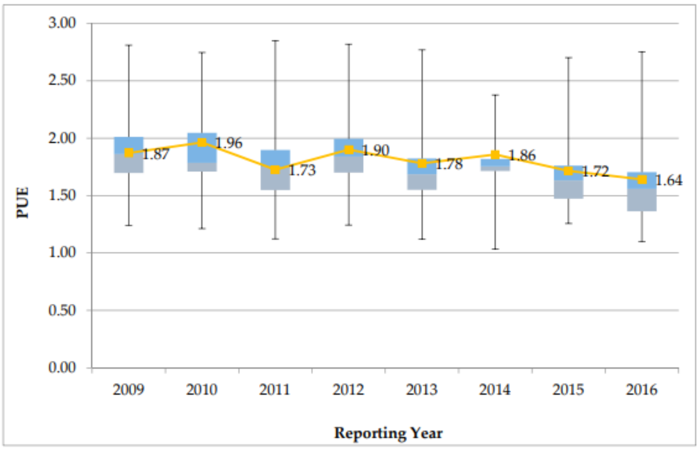


Figure 10 Average PUE per Reporting year, Source: Trends in European Data Centre Energy Consumption (Averingou et al 2017)

obvious financial benefits by reducing the PUE and as such, it is reasonable to assume these systems are optimised where possible. Cooler climates clearly offer an advantage in terms of reducing cooling requirements, however the approaches and reductions achieved appear sensationalised in some instances either by media or for marketing. It appears unlikely that a PUE of 1.05 is achievable for the average miner, especially through the use of air cooling alone. If this rate was feasible it would be unlikely that several industry leaders would implement techniques such as immersion cooling as the associated costs of implementing such techniques would be unnecessarily costly in comparison to the use of air cooling in most instances.

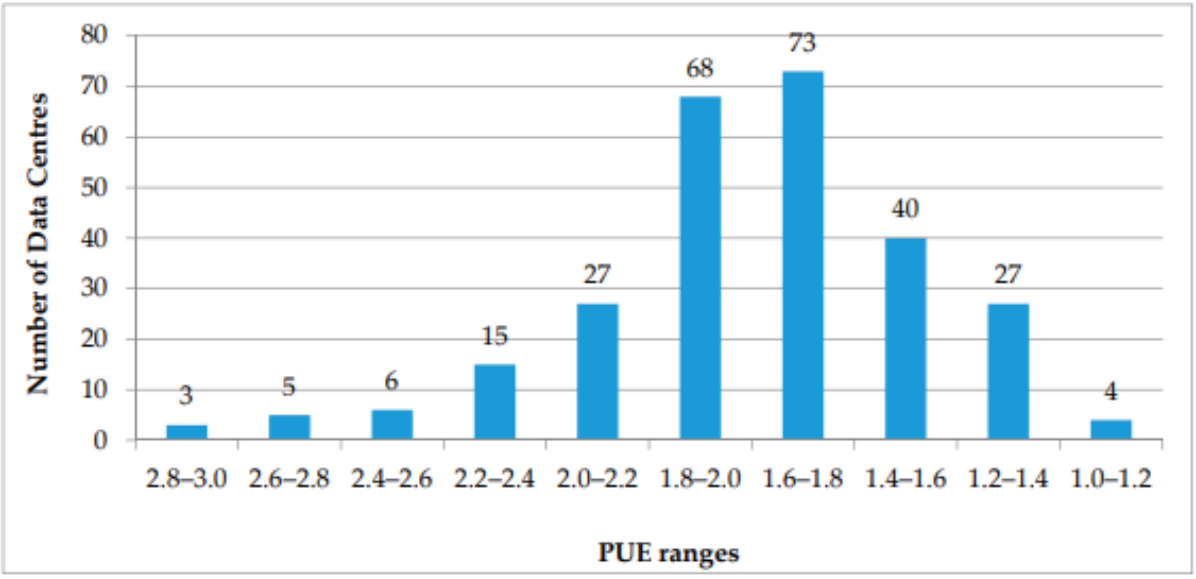


Figure 11 Number of Data Centres in Each Range within Europe, Source: Trends in European Data Centre Energy Consumption ((Averingou et al 2017)

4.5Global Electricity Prices

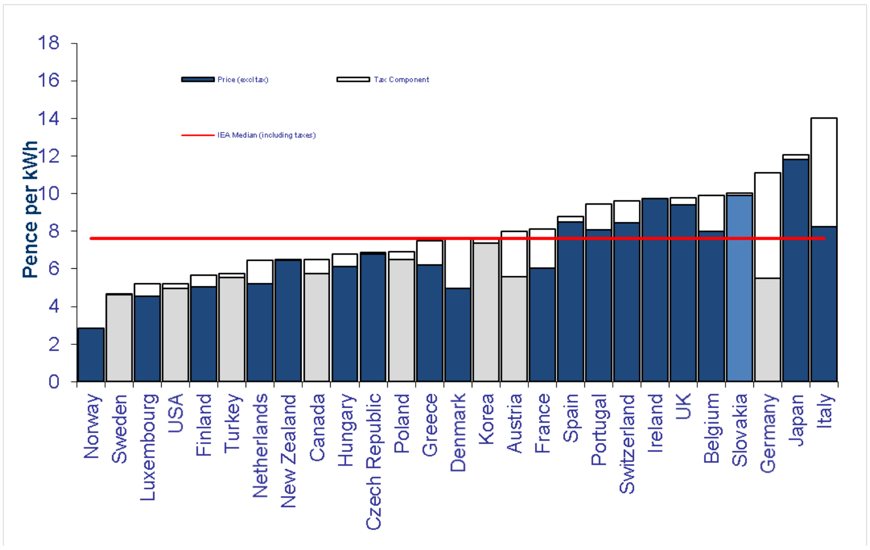


Figure 12 Average Industrial Electricity Prices, International Energy Agency 2018 Statistics

Previous energy estimations have rallied around the figure of $0.05 per KWh with little justification given to why this figure is used. There also appears to be no consideration given to the differing costs in regional electricity prices, or the reduced rates that most industrial consumers negotiate with suppliers. Reviewing the IEA statistics and considering the location, known prices paid and offered this figure requires further investigation and validation. As figure 9 highlights the average industrial energy price per KWh indicates a median of 7.28p per KWh. However, this figure omits the typical industrial prices paid in China and Iceland two major hubs of industrial mining farms. It is also important to consider that mining operations seek out countries and suppliers with low energy prices, and that energy prices displayed are unlikely to indicate the price paid by industrial mining operations. North American Giga-Watt mining offer data centre's electricity at a rate of $0.028 KWh[24], Norway whom have numerous large scale operations offer a rate of $0.03 per KWh[25], and Jhian Wu Bitmain CEO has confirmed that the world's largest mine (Oros Inner Mongolia) receives electricity at a rate of $0.04 per KWh[26]. The sources or primary generation methods in the regions of these mining operations should also be analysed. All the largest mining facilities operate in regions where there is an abundance of hydroelectric, wind, or geothermal electrical generation suggesting that industrial scale miners are already focused on low cost renewables, reducing their carbon footprint and increasing sustainability.

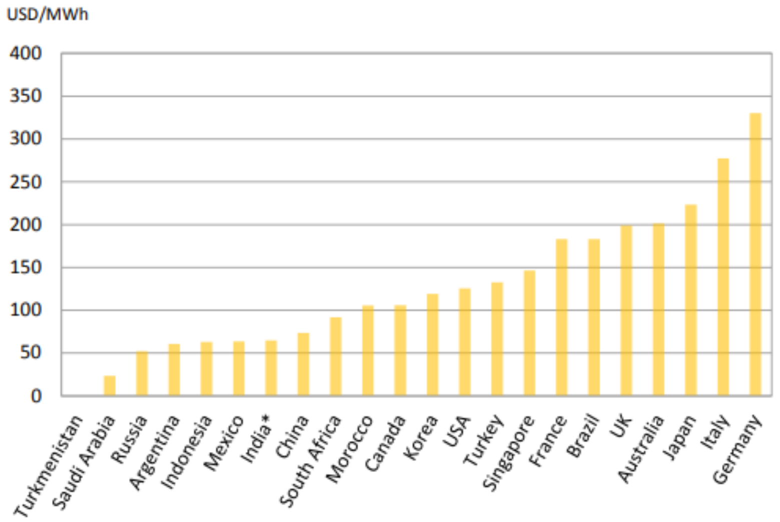


Figure 13 World Energy Price Statistics, Source: International Energy Agency 2018 Overview

4.7 Part B – Growth Analysis

Investigation in to historic energy demand of the bitcoin network found that previous research by (Dwyer& Malone, 2014)[27] had

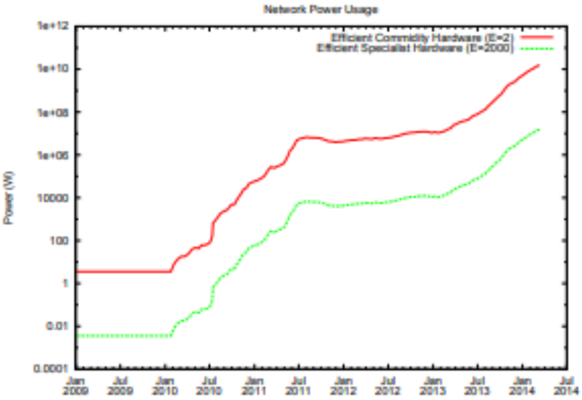


Figure 14 Estimated Power Consumption of the Bitcoin Network, Source: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6912770

used a similar methodology and identified the energy demand of the Bitcoin network to that utilised with this paper and more closely to that of Alex de Vries. During this period FPGA were the primary equipment utilised in the mining process. The results of their work indicate that prior to the introduction of ASIC's the bitcoin networks energy demand was greater in July 2014 than it is currently. This was during a previous all-time Bitcoin price high and subsequent major correction, but suggest that when the upper limits of FPGA efficiency were reached a significant increase in energy demand occurred, while the introduction of ASIC and the subsequent efficiency increase of overall mining equipment had a significant effect on reducing the network energy requirements the following year.

4.7.2 ASIC Progression

Increasing equipment efficiency has in part driven the exponential increasing in network hash rate of Bitcoin. When considering the future energy requirements of a system such as PoW it is critical that the limitations of the equipment are also considered as. Gordon Moore's co-founder of Fairchild semiconductors and Intel suggested in his 1965 paper that the number of transistors in an integrated circuit board doubles approximately every two years.[28] This has been established as Moore's Law, and once the upper limits of transistor physical capabilities are reached it is likely to impact ASIC chips and thus PoW mining and the electricity demand of the network. Current industry leading ASIC chip manufacturers have achieved transistor gate sizes of 7nm.[29] Silicon the main material used to construct transistors has an atomic size is 0.2nm, suggesting the upper limits of this from of hardware in terms of efficiency increase are approaching. Investigation and analysis of the ASIC progression is key in making accurate future estimations of the network electricity demand.

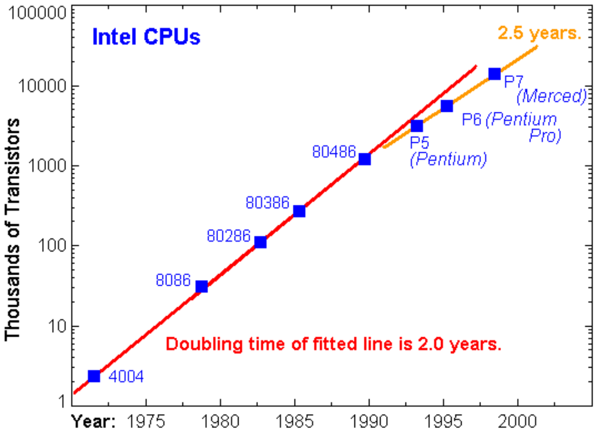


Figure 15 CPU Transistor Size Progression, Source:https://www.tf.uni-kiel.de/matwis/amat/semitech_en/kap_5/backbone/r5_3_1.html

4.8 Part C – Comparison of Financial Systems

4.8.1 Hass McCook- An Order-of-Magnitude Estimate of the Relative Sustainability of the Bitcoin Network [30]

The work presented by (McCook, 2014) highlights some of the possible socio economic benefits of this technology including the ability to reduce fraud and does well to set out a first order methodology of the economic implications. The work does well to estimate the energy demand of the current financial systems as well as the energy demand of the fiat currency minting process which appears thorough with robust and known data being extrapolated proportionately in order to establish global figures. It does well to establish base case scenarios for economic and environmental implications of the financial system, however a slightly biased tone towards Bitcoin throughout leads to scepticism and as such the figures were approached with caution. By assuming bank branches utilise a similar amount of energy McCook has managed to reach a reasonable base figure for the energy requirements of the global banking network. Estimations on ATMs aligned with the author's own research, calculations, and the available empirical data, and will be used in comparisons within later parts of this thesis where appropriate. Estimations on associated CO2 will not be included due to the lack of clarity on generation sources, and the possibility for inaccurate and misleading results.

One metric that will be adopted to compare the efficiency of the differing fiscal systems is the KWh per transaction metrics utilised by De Vries. An attempt to expand on this give a more accurate context to the findings will also be required. De Vries only makes one comparison in his paper, and due to the nature of how visa net operates the information presented can be misleading. Visa net the platform on which visa transactions take place on does not operate on its own, and similarly to the Lightning Network proposal of Bitcoin requires a network of computers, servers, banks, ATMS and Point of Sale devices to operate. By expanding on this work, a more accurate comparison of the sustainability of these systems can be made.

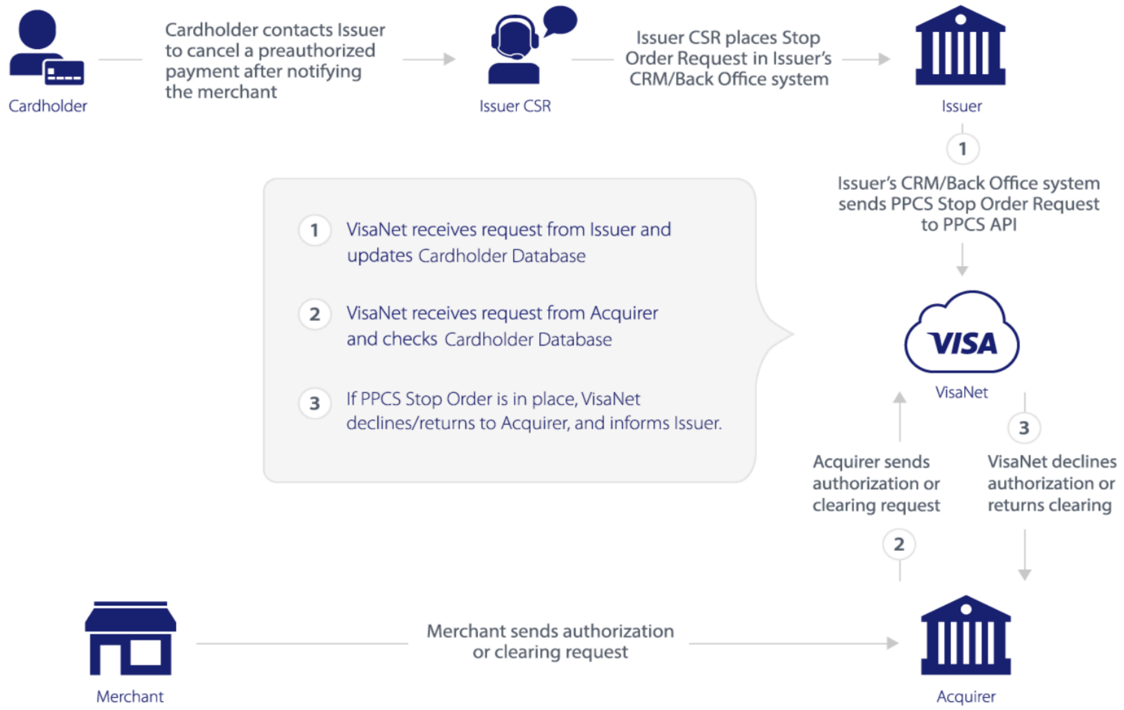
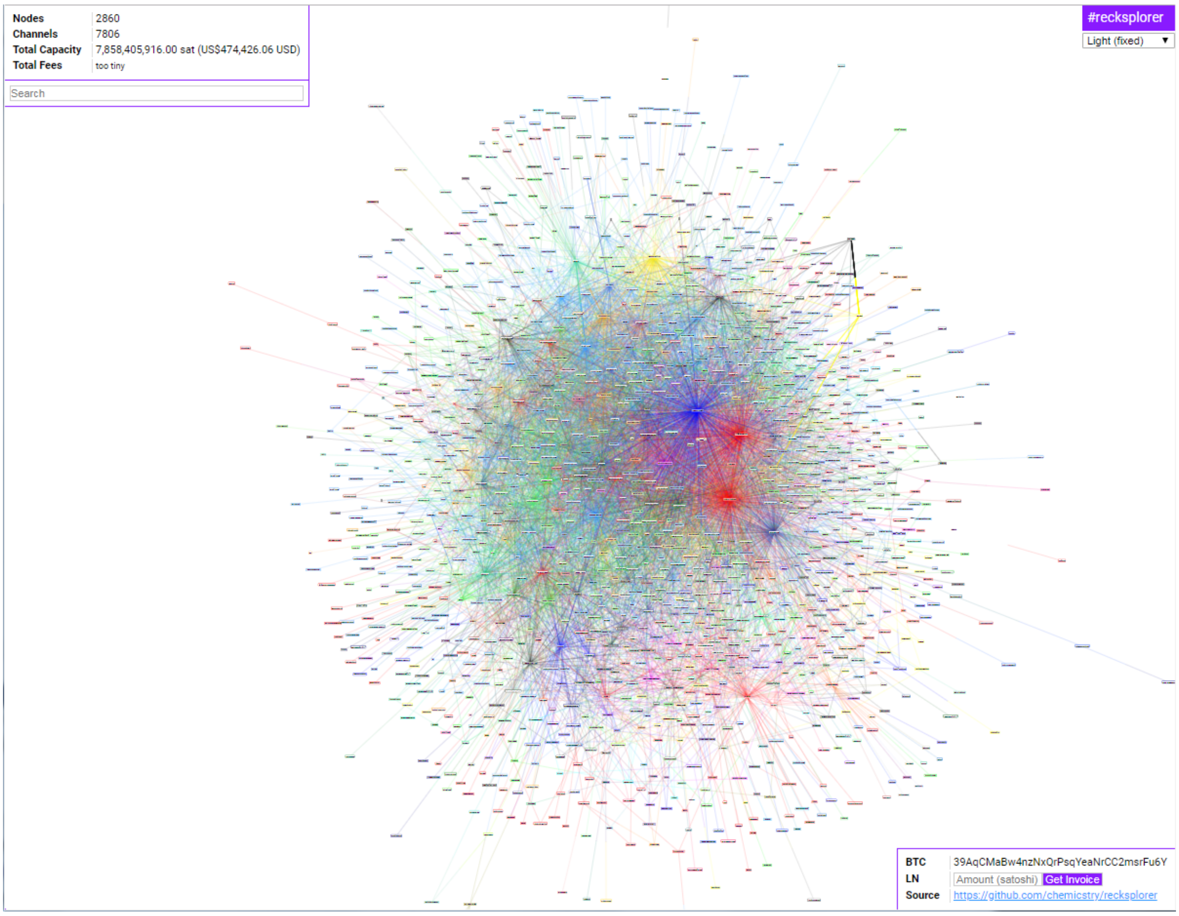


Figure 16 Visa Net Operational Model: Source: https://developer.visa.com/capabilities/ppcs/docs

4.8.2 Lightning Network

An average of 3 to 4 transactions per second are currently taking place on the Bitcoin Blockchain with an upper limit of 7tx per second.[31] With well over a billion non cash based Tx occurring globally every second there is a clear scalability problem.[32] The Lightning Network proposes a solution to this through the creation of a second layer PoS based system with bidirectional payment channels being setup between nodes within the eco system.[33] As this proposal is currently in the Beta testing phase and currently has just over 2000 nodes, the overall viability is yet to be clarified. [34]



Nodes 2860
Channels 7806
Total Capacity 7,858,405,916.00 sat (US$474,426.06 USD)
Total Fees too tiny

BTC 39AqCMaBw4nzNxQrPsqYeaNrCC2msrFu6Y
LN Amount (satoshi)
Source https://github.com/chemicstry/recksplorer

Figure 17 Visualisation of Lightning Network Nodes, Source: https://lnmainnet.gaben.win/

The metrics used to measure the networks progress is recorder in number of nodes and the transaction capacity in BTC or $ creating difficulty in estimating the volume of transactions occurring in the network. Estimating the overall energy demand of the network can be achieved through an estimation of average node electricity consumption, however it should be considered that these nodes were more than likely already operational and consuming power despite their current interaction with the Lightning Network and as such should ould be considered negligible.

4.9 Literature Conclusion

Overall there are few but significant difference in methodologies utilised by Bevand and De Vries, both are based on the economics and profitability of mining and use the same cost per KWh for their assumptions. Both have shortcomings that are briefly mentioned but not addressed in full such as general assumptions on data centre PUE, there is no indication or justification of how electricity costs were estimated or the impact of varying electricity prices and the knock on effect this has on the profitability threshold assumption and finally the likely hardware implemented in the mining process. The economic based approach considering hardware costs, results in a significant and arguably inaccurate increase in energy requirement estimations. This appears flawed due to the varying price, profitability and potential that the resale of equipment can have, or as highlighted by De Vries himself the irrational or hobbiest minor not complying with the profitability assumption.

There is a large gap between the PUE estimations of Morgan Stanley and those reached by independent reports. Investigation indicates that the figures utilised by Morgan Stanley match and are most likely taken from the estimates reached by (Averingou et al, 2017). They do not consider the aggressive optimisation that mining operations seek, while it is also important to consider that while some leading operations achieve a PUE of 1.05 that many of the smaller less refined operations will likely not achieve such efficiency increases . Verifying and improving the accuracy these parameters would appear to be an essential aspect of making accurate estimations of the network energy consumption. Taking the median values of the known electricity and PUE data appears to be most accurate means of estimating these figures for use as the weighted average is unlikely to be accurate due to a lack of data regarding mine size and location.

Independent analysis of Morgan Stanley's BITMAIN estimations indicate that the output figures generated raise question about the reliability of their data and methodology, or that there are external factors that have not been considered.

Morgan Stanley Data Analysis	
Number of Antminer S9 Network Requires	2169664.879
Morgan Stanley Estimated S9 Production	6000000
Number of S9 in Excess	3830335.121

Table 1 Analysis of Morgan Stanley Bitmain Findings

As table 1 highlights, the output estimations suggest that there are currently 6 million Antminer S9 in circulation, while the total number of S9 required to support the entire network is 2.2 million leaving an excess of 3.8 million Antminer S9 produced. As the life span/profitability of this hardware is time constrained and generates the greatest profits in the earliest stages of its life it is highly unlikely that this volume of units are sitting idle, in transport or damaged. The analysis indicates that these figures are an over estimate and that Bitmain most likely use the same chips in other mining hardware manufactured for alternate crypto currency mining equipment. However their estimation that Bitmain products have 70% share of the ASIC market does appear to be valid as the figures revealed from their closest rivals Canaan suggest their mining equipment accounts for a 22% share of the total hashrate [23], while other close rivals GMO account for only 1.34%. Justification for these figures are essential in improving the accuracy and reaching consensus in energy consumption estimations, with the median PUE being 1.34, and the median electricity price is $0.051 validating the electricity price used in previous estimations.

The energy demand estimations reached by (Dwyer and Malone, 2014) revealed valuable historical data, and allows for a basis in estimating the impact of reaching the upper limits of ASIC efficiency. The work conducted by McCook offers a robust methodology to base further work, as stated CO2 estimations should be approached with caution due to the lack of clarity over energy sourcing. Preferably alternate data sources can be found of the legacy banking systems energy impact that can validated estimations reached.

5 Methodology

5.1 PART A- Proof of Work Energy Estimations Tool Development

5.1.1. ASIC Hardware Statistics

Using Excel Spreadsheet, the first step in developing energy estimations tool is to compile a list of the viable mining ASIC. In previous estimations a short list of the most recent and efficient hardware is made and is the basis for further calculations. By compiling a more comprehensive list of all current and previously available hardware that has or will reach the market, a greater accuracy and more realistic output can be achieved. The release date, capacity in GH/s, efficiency in J/GH, and power consumption of each unit are also logged. In order to ensure the list is comprehensive it has been cross referenced with previous estimations , ASIC manufacturer's websites and external directories.[34]

Table 2 Example of Tools Successful Mining Chips Table

Overview of successful ASIC Mining Chips

Release Date	Manufacturer	Model	TH/s	Watts	J/GH	Mh/J	Estimated Gate size nm
28/12/2012	ASIC Miner	BE100	0.000336	2.016	6	167	130
20/01/2013	Avalon	A3256	0.000295	1.947	6.6	152	110
08/02/2013	Butterfly Labs	Bitforce SC	0.0042	12	2.857	350	28
14/06/2013	Bitfury	BF756C55	0.002675	2.0875	0.78	1281	55
01/08/2013	ASICrising GmbH	WolfBlood	0.00912	5.928	0.65	1538	28
01/08/2013	Avalon	A3255	0.0015	2.4	1.6	625	55

This process has been repeated with the known ASIC mining chips that have been manufactured and successfully reached the market.[35] The release date, power consumption, efficiency, hash rate and estimated gate size have all be logged. The data has then been sorted by release date in order for any trends in efficiency and transistor gate size to be identified. While this second table is not required in making initial estimations, understanding the trends within mining ASIC are essential for future estimations with the efficiency, power consumption and hashing ability of hardware constantly evolving.

Overview of Mining Hardware that reached Market

Release Date	Miner	Capacity GH/s	Efficiency J/GH	Price $	Power Consumption W
06/04/2013	AntMiner S1	180	2	299.00	470
	AntMiner S2	1000	1.1	2259	1100
	AntMiner S3	441	0.77	382	1186
	AntMiner S4	2000	0.7	1400	1450
	AntMiner S5	1155	0.51	370	590
	AntMiner S5+	7722	0.44	2307	3436
	AntMiner S7	47300	0.25	479.95	1300
	AntMiner S9	13500	0.098	1,987.95	1320
01/03/2018	AntMiner V9	4000	0.257	199	1027

Table 3 Example of Tools Mining Equipment That Made it to Market Table

5.1.2. Profitability Table

The second step in the tool development is to create a table of the daily profitability of each mining ASIC. First the price of the PoW currency, the network difficulty, and the block reward must be imported from external data sources using API keys.[36][37] The median electricity cost paid was found to be $0.051 KWh and has been used in the estimation as this aligns with previous estimations allowing for empirical validation of the tool results and after independent investigation found to be a reasonable estimation of the global whole sale price of electricity supplied to industrial Blockchain mining applications. In order to estimate the daily profitability the average daily reward in bitcoin of each ASIC were estimated using the following equation:

$$\boldsymbol{Daily\ Reward\ (Bitcoin)} = \frac{\boldsymbol{Unit\ Hash\ Rate * Reward\ per\ Block * 86400 * 1000}}{\frac{\boldsymbol{Difficulty * 2^{32}}}{\boldsymbol{600}}}$$

This Reward is then exchanged for the US Dollar equivalent, and the daily electricity costs have been subtracted in order to establish if each mining ASIC is profitable or not, and then colour coded to allow for easier indication of the viable hardware.

5.1.3. Network Hardware Breakdown

Once again, an external data source is required, and the total network hash rate must be imported in order to establish the network breakdown on any given day. A new table has been created of 'possible network hardware'. Using excel functions Vlookup and data sorting it identifies which hardware in the profitability table is economically viable based on current network conditions, and automatically assembles a list of the hardware, their efficiency, capacity and power consumption. A second table is created that lists the weighted average of each ASIC based on market share from the available data.

Total> Network Hash Rate GH/s	42,733,900,000.00	42,733,900.00	**<Total Network Hash Rate TH/s**
Possible Hardware in Network			
Mining Hardware	**Viable Network Efficiencies J/GH**	**Capacity GH/s**	**Power Consumption W**
AntMiner S1	0	0	0
AntMiner S2	0	0	0
AntMiner S3	0	0	0
AntMiner S4	0	0	0
AntMiner S5	0	0	0
AntMiner S5+	0	0	0
AntMiner S7	0.25	47300	1300
AntMiner S9	0.098	13500	1320
AntMiner V9	0	0	0
AntMiner T9	0.126	12500	1576

Table 4 Example of Tools Viable Hardware Table

A third table was then created of 'The Network Hardware Outputs and Statistics'. This table identifies and includes the most and least efficient possible hardware as well as a median and weighted average efficiencies. It then identifies the number of required ASIC within the network and the typical power consumption of each unit based on the current network hash rate and outputs of the previous tables.

5.1.4 Network Energy Requirements

A fourth sheet was then created with a table to indicate the ‘Current Network Energy Requirements’. Here the outputs and results of the previous sheets are converted into a demand capacity in Mega Watts, this has been extrapolated into daily electrical demand in TWh and an annual demand TWh/yr. The median PUE of 1.36, estimated from the literature review investigation has then been accounted for to give a more accurate indication of the overall energy requirements of the network. The final daily demand is then converted to an annual demand in Twh/yr and finally as a percentage of annual global and renewable electricity generation based on IEA headline electrical generation statistics.[38]

5.1.5 Global Energy Impact Tables

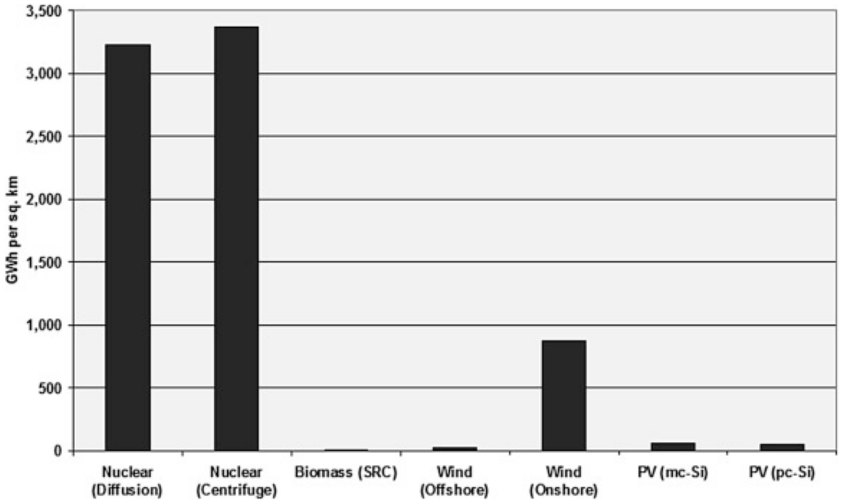


Figure 18 Energy Density per Km2 by Generation Type, Source:https://www.researchgate.net/profile/Geoffrey_Hammond2/publication/271724019_Energy_Density_and_Spatial_Footprints_of_Various_Electrical_Power_Systems/links/55f55bfa08ae6a34f660d3a0.pdf

Several output tables were made to quantify and to make comparison of the energy required by the Bitcoin network. Using the latest IEA data on global electricity production, a table was created to indicate the percentage of each Nations annual electricity generation required to power the Bitcoin network. The table also indicates the percentage of each nation’s fossil fuel, renewable and nuclear generation deployment required to support the network based on the daily statistics. A second table was then created to indicate the impact of the Bitcoin network on the world’s largest electricity generators by fuel source. Should the asset not be capable of supporting the entire network the table also highlights the comparable area required based on the power density of the asset and its area covered in km^2.

The area required to support the Bitcoin network based on various generation methods has also been estimated. The power density figures of varying generation methods (GWh/km^2) reached by (Cheng, Hammond et all, 2014)[39] have been adopted in order to estimate the new deployment area required of each generation method.

5.2. Part B – Growth Analysis

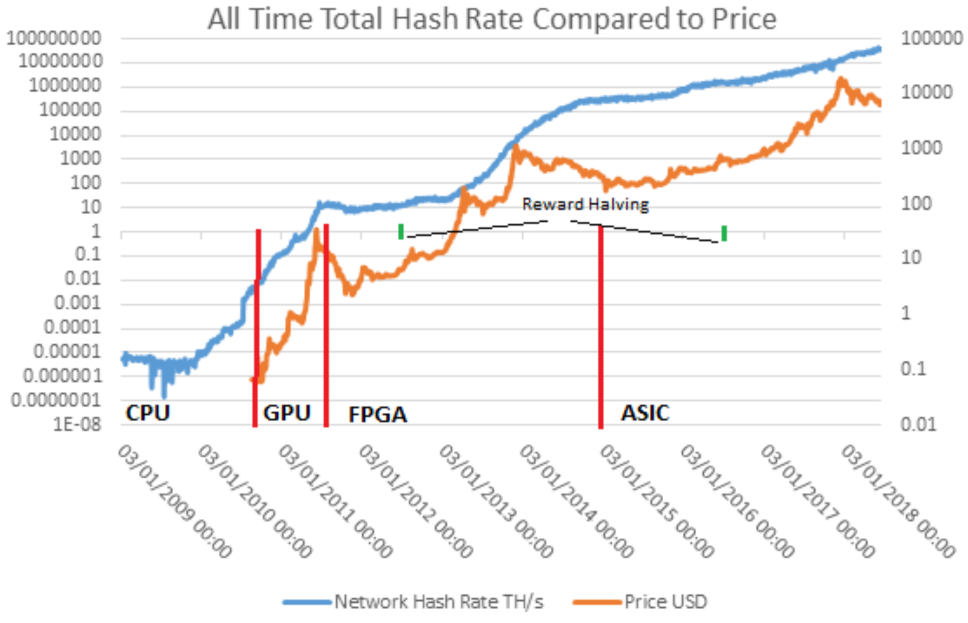


Figure 19 All Time Hash Rate and Price Growth Comparison

When analysing the logarithmic scale of all-time network hash rate and price trends, combined with major events that will affect the mining process included such as reward halving or the introduction new hardware several trends become clearer. Rapid increase in price can be seen forming a corrective wave down on three occasions shortly after the value comes within proximity of the hash rate trend line. It can be seen that soon after the mining reward is halved the price tends to increase, most likely down to the reduction in supply as previously discussed generating inflation. Second, that towards the end of each equipment cycle the total network hash rate increases are greatest then followed by a curtailment of hash rate expansion, similar to an asymptotic top before continuing to rise once again. This highlights the impact of the leading mining equipment reaching the upper limit of possible efficiency increases and how it will impact the total network hash rate in future, these considerations will be important in making forecasts of the networks future electrical demand.

Forecasting of three possible paths of the bitcoin price and network have been estimated. A continuation of the current/historic growth rate, a stabilised and continued growth and a decline in growth. In order to make estimations it has been assumed that ASIC will continue to be the primary mining equipment, and that developments in ASIC efficiency, power consumption and hash rate will adhere to the results found within the ASIC progression analysis. An addition ASIC was added to the profitability table with the specifications estimated from the analysis, it will also assumed that the most efficient equipment will be used and as such results from the best case scenario have been used in these forecasts. In order to ensure accurate estimations were achieved the difficulty equation below was used, and the reward halving has been also been implemented.

$$Difficulty = \frac{hashrate}{\left(\frac{\frac{2^{\wedge}256}{Tmax}}{Intended\ Time\ per\ Block}\right)}$$

5.3. Part C – Comparison of financial Systems

Data has been collected and compiled from numerous payment and daily transaction sources, including Visa, Link ATMs and Point of Sale devices. There are 69.6 thousand Link ATMS in UK[40] with 3.105 billion tranactions occurring per annum. Figures on the typical power consumption per ATM have been taken from (Roth et al, 2002)[41].These figures align with the work by McCook verifying the outputs achieved. UK point of sales terminal data was also gathered.[42][43] Visa statistics were taken from their annual Corporate Responsibility Report, and information requests were submitted to both Paypal and Mastercard however, no response was received from either.[44] A comparison of the electricity demand of global minting process was made using a combination of the data sourced independently and form (McCook, 2014) with total end energy demand being converted to KWh to make accurate comparisons. Estimates of Global transactions per KWh, total network demand and minting process being estimated.

6 Results

6.1. Part A - Energy Estimations Tool Results

6.1.1. Current Energy Requirements Table

The range of output in the table of results produced by the model highlights the uncertainty over generating energy estimations. The most and least efficient outputs have been empirically validated through comparison with estimations made by Marc Bevand. The weighted average output is the most probable scenario and as such was used for all further comparisons and metrics

Current Bitcoin Network Energy Requirements				
	Most Efficient	**Least Efficient**	**Median**	**Weighted Average**
Power Capacity MW	2674.65	6407.18	2480.07	3839.68
Daily Electrical Demand TWh	0.06	0.154	0.060	0.092
Annual Electrical Demand TWh/yr	23.43	56.13	21.73	33.64
% Annual Global Electricity Generation	0.10%	0.231%	0.090%	0.14%
% Annual Global Renewable Generation	0.42%	190%	0.39%	0.61%
With PUE consideration of 1.36				
Power Consumption MW	3637.52	8713.76	3372.89	5221.97
Daily Electrical Demand TWh	0.087	0.209	0.081	0.125
Annual Electrical Demand TWh/yr	31.865	76.333	29.547	45.744
% Global Electricity Generation	0.13%	0.31%	0.12%	0.189%
% Global Renewable Generation	0.58%	1.38%	0.53%	0.827%

Table 5 Network Electrical Demand Output Table

In order to make relevant comparisons the largest energy generation assets by source have been listed and the portion of each assets output required to power the bitcoin network have been calculated with the inclusion of each assets capacity factor to ensure more accurate figures were achieved. As can be seen in table 6 the electrical draw of the network currently requires 52% of the three gorges dam output, and requires the equivalent area of $20km^2$. The Rance Tidal system however would need to be 2728% larger to power the entire bitcoin network. The comparable area required column highlights the energy density of differing generation methods. The inclusion of a capacity factor and its impact on the portion of asset required column highlights some of the challenges faced by many generation methods in supplying consistent base loads and the large areas they required. While density varies with location the impact on these individual assets gives a realistic indication of the required area should the network be powered exclusively by a single generation source and location.

Impact on World's Largest Energy Assets

Location	Installed Capacity MW	Generation Type	Portion of Asset Required	Area Required to support Bitcoin Network km2
Three Gorges Damn	22500	Hydro	52%	20.3
Gansu Wind Farm	7950	Onshore Wind	199%	N/A
Bruce Nulcear Canada	6384	Nuclear	91%	8.5
Surgut 2	5597	Gas CHP	167%	1.4
Tengger Solar Park	1547	Solar PV	545%	604.8
The Geysers Geothermal	1520	Geothermal	1764%	425.3
London Array	630	Offshore Wind	2728%	2151.6
Noor Concentrated Solar	580	Concentrated Solar	7771%	68.2
Rance Tidal	240	Tidal	2728%	1748.4

Table 6 Portion of Individual Energy Asset Required to Support Bitcoin Network

Tables 6 and 7 put the network electrical demand into context from a national or individual generating asset perspective. Table 7 indicates the % of each nations fossil fuel, nuclear or renewables deployment required to support the network. Hypothetically a DDoS attack requires 51% control of a network, when the electrical requirement of such an attack are considered it is clear that it would require a small % of most larger nations electrical output, and only a fraction of a single generation sites outputs to facilitate such action. This highlights that the network is still vulnerability from an attack by nation state such as America or China from an energy standpoint.

Country/Source	Product	Electrical Output GWh (2015)	% of Deployment Required
Australia	Fossil fuels	217871	21%
Australia	Nuclear	0	0%
Australia	Renewable sources	34405	133%
Australia	Total	252276	18%
Austria	Fossil fuels	13725	333%
Austria	Nuclear	0	0%
Austria	Renewable sources	47243	97%
Austria	Total	61763	74%
Belgium	Fossil fuels	27273	168%
Belgium	Nuclear	26103	175%
Belgium	Renewable sources	14466	316%
Belgium	Total	69548	66%
Canada	Fossil fuels	141306	32%
Canada	Nuclear	101423	45%
Canada	Renewable sources	422643	11%
Canada	Total	670740	7%

Table 7 Required Portion of Existing National Electrical Generation to

Support the Bitcoin Network

6.1.2. Required New Deployment

Using the spatial density of differing generation methods, the area currently required to support the network by generation type has been estimated. The results indicate that currently the total area required to support the network is well below 1 km^2 for several generation methods.

Required Electrical Generation Deployment of Bitcoin Network					
Generation Method	**Nuclear**	**Solar PV**	**Wind Offshore**	**Wind Onshore**	**Biomass**
Average Power Density GWh/km2	3233.00	61.84	22.64	872.4	2.13
Area Required km2	0.0016	0.0844	0.2307	0.0060	2.4516

Table 8 Required New Electrical Generation Deployment to support Current Network

6.1.3. ASIC Daily Modelling Results of Network Demand

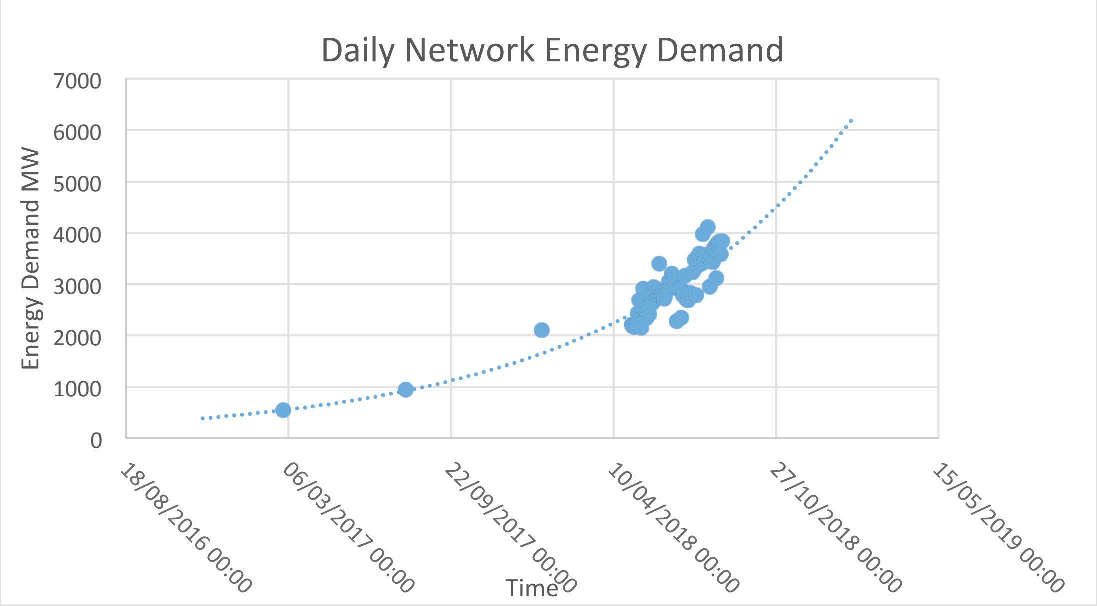


Figure 20 Daily Modelling Results over Time

The results from monitoring the models daily energy demand were combined with the historic results achieved by Marc Bevand. Analysis of these results confirms that the current growth in hash rate is systemic and that the energy demand is currently increasing exponentially. The daily results generated highlight that while price has declined the energy demand of the network has almost doubled during this time from just over 2000MW to 3800MW.

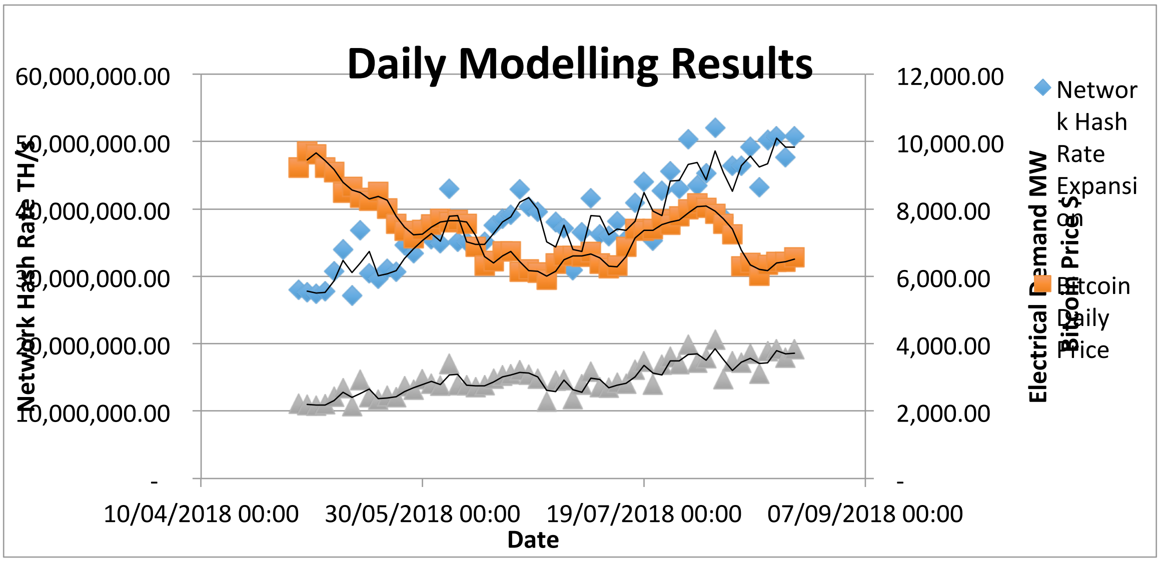


Figure 21 Daily Modelling Results Compared to Price and Hash Rate

6.2. Part B – Growth Analysis Results

6.2.1. ASIC Efficiency and Gate Size Analysis

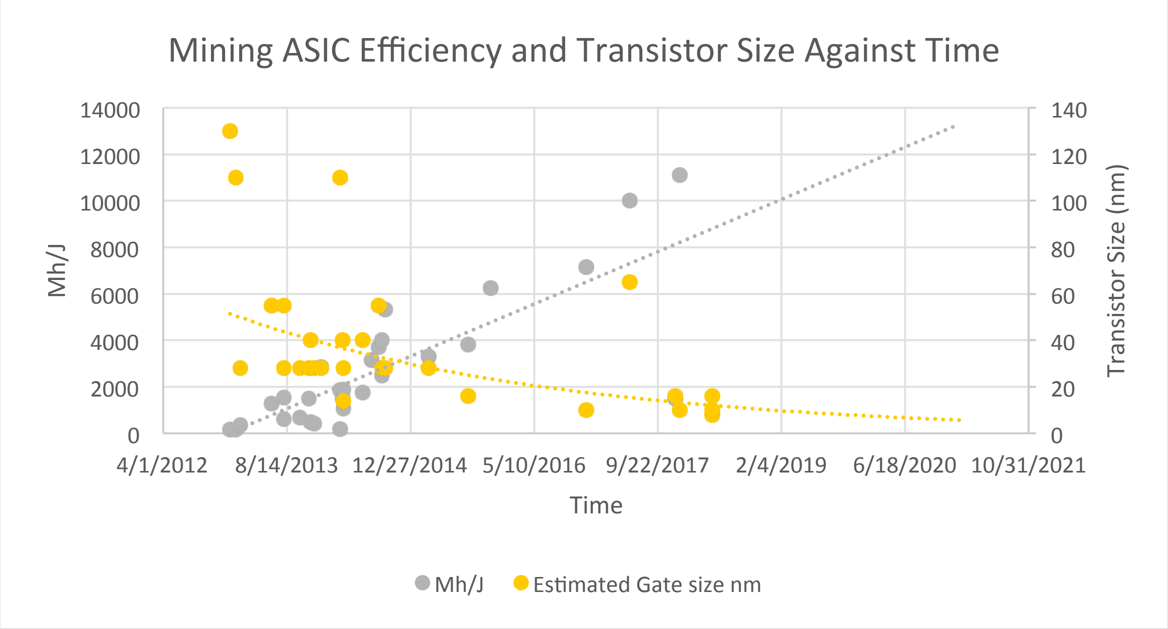


Figure 22 ASIC Mining Chip Transistor Progression Results

Results from the analysis of trends within ASIC chip developed for SHA256 mining equipment found that the increasing energy efficiency of transistors adheres to Moore's law of transistor density and efficiency increases. By fitting a line of best fit, it can be seen that if current trends continue the physical limits of silicon (1nm diameter transistor) ASIC equipment will be reached in June 2020. With an estimated 12000 MH/J being achieved should current trends continue.

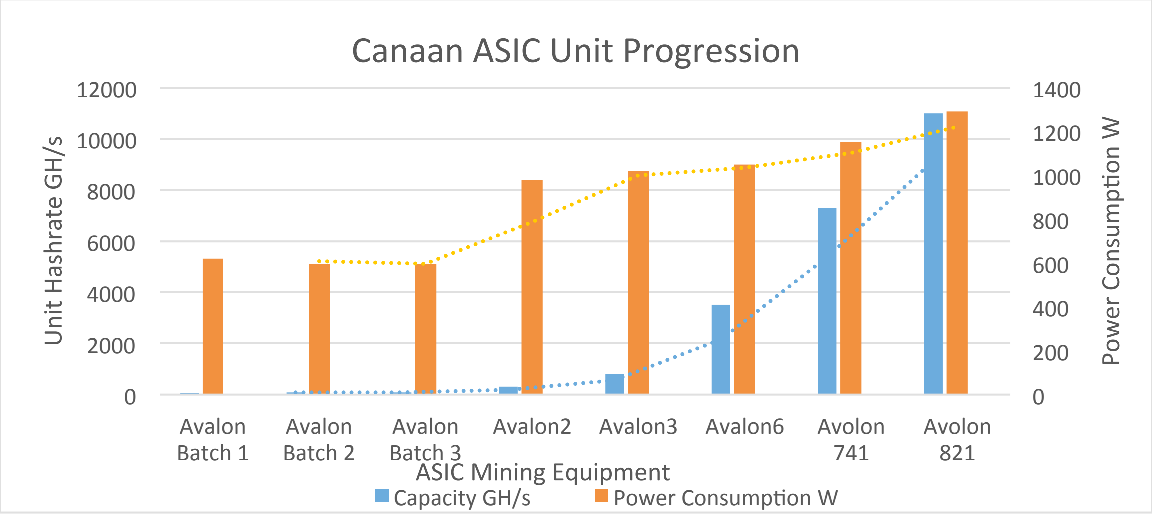


Figure 23 Canaan ASIC Mining Unit Hash Rate and Power Consumption Progression over Time

Analysis of the progression trends within the ASIC mining units found that while the chips implemented with each generation are reducing in size the overall shape and size of each unit has been somewhat standardised. This has caused the number of chips within each unit to increase despite the increasing chip efficiency. As Figures 20 and 21 highlight this has resulted in exponential growth in the hashing capacity but also an overall growth in the Power consumption of each unit.

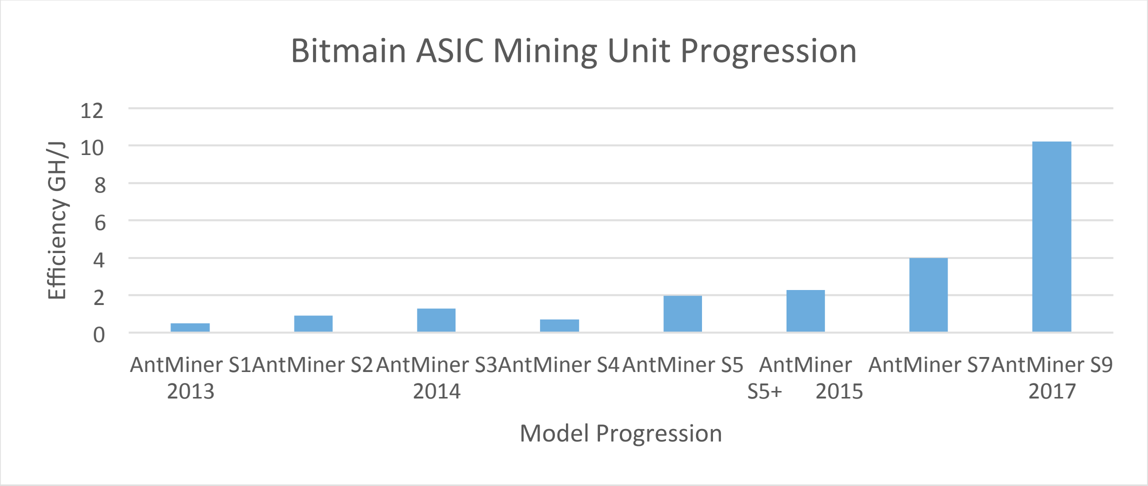


Figure 24 Bitmain AISC Unit Efficiency Progressions

6.2.2. Market Price, Hash Rate Trends and their Energy Impact

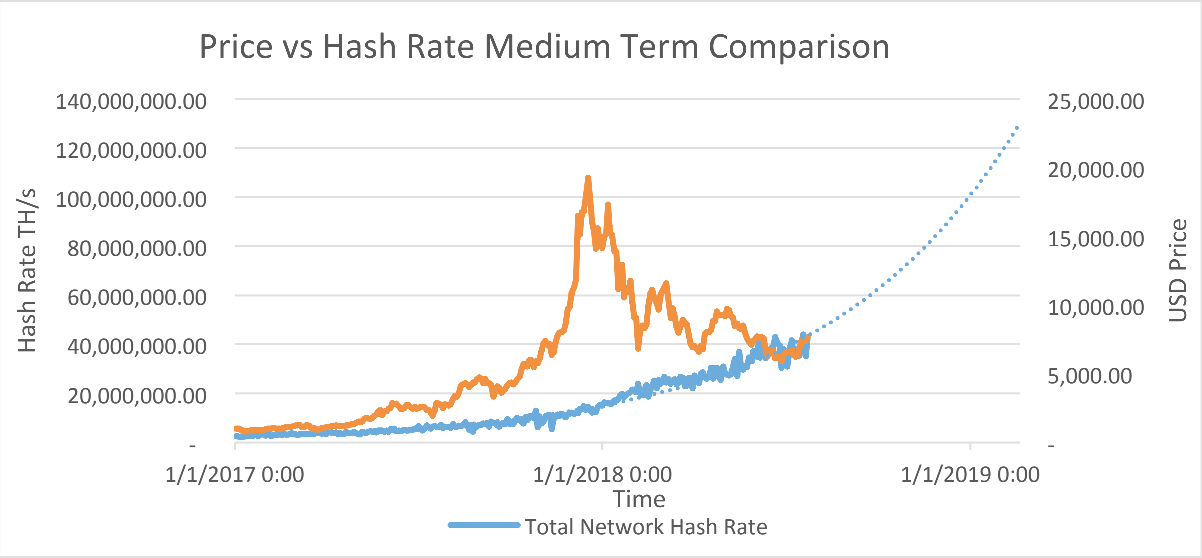


Figure 25 Medium Term Price and Hash Rate Growth Comparison

Analysis of the medium term market trends indicates that the despite the down turn in price over the previous 6 months the total network hash rate has continued to increase exponentially. A small spike in hash rate during February highlights that sudden price increases also impacts on hash rate dedicated to the network.

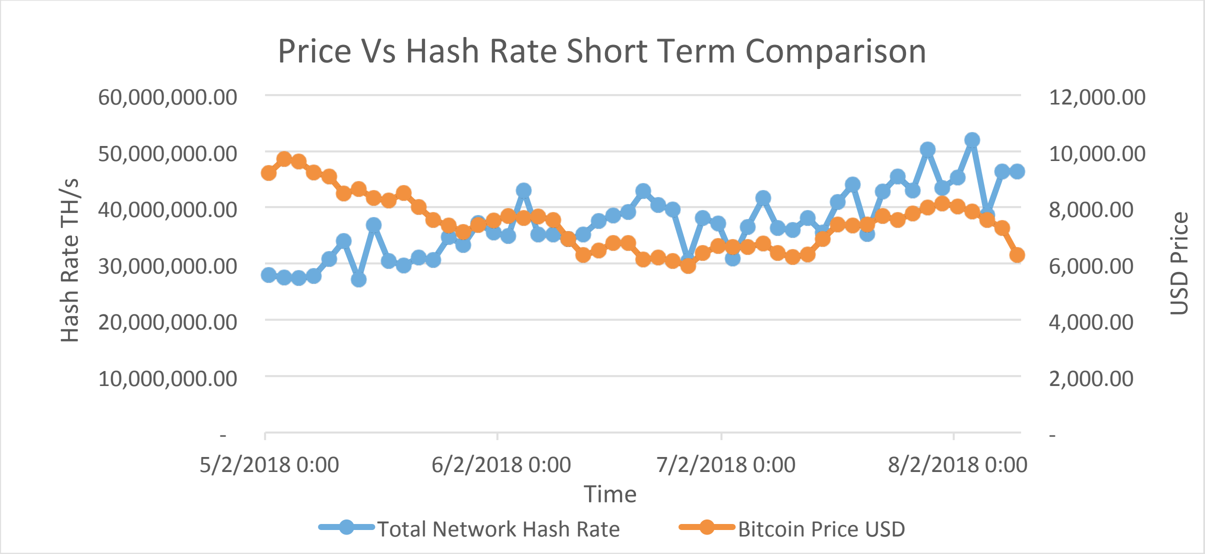


Figure 26 Short Term Price and Hash Rate Growth Comparison

Review of the short-term price and hash rate trends highlights that the overall trend of the hash rate can be seen to increase while the price reaches a bottom and then starts to regain value. Small daily spikes in hash rate appear to correlate in part to daily price spikes, it can be argued that this indicates price increases likely impact sentiment and as such will likely cause an increase in total network hash rate as miners whom mine the most profitable currency on a daily basis turn their focus back to Bitcoin.

6.2.3. Historic Energy Demand

Analysis of historic energy estimations found interesting results. As discussed in the literature review, the energy demand of the network in

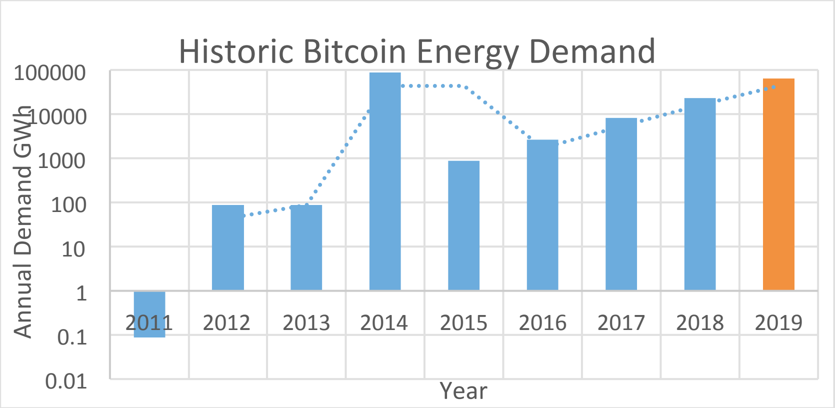


Figure 27 Yearly Bitcoin Energy Demand

2014 was greater than current requirements, the upgrading of hardware to ASIC's had a significant impact on reducing the energy demand of the network. However the upper limits of their efficiency is approaching, and could cause significant increases in energy demand as were seen in 2014. The 2019 estimation have been generated by extrapolating the trend line from the daily modelling results with the assumption that ASIC's will continue to dominate the market and that their efficiency increase will be within the bounds estimated in figure 19. Beyond this point, estimations are more challenging due to the lack of certainty over ASIC progressions, network hash rate and BTC price.

6.2.4. Possible Future Trends

It is difficult to accurately estimate future trends in any market, and thus in order to make viable long-term projections of the network energy demand three possible trend lines have been added. A continuation of the all-time trend, a stabilized growth trend and a price decline trend. Stabilised growth and a price decline would likely result in a reduced impact on global energy networks in comparison to a continuation of the current trend. From an energy perspective, the continuation of the all-time trend would likely have significant ramifications and as such it will considered a worst case scenario and its potential impact on global energy will be this documents focus. In order to establish estimations of the networks

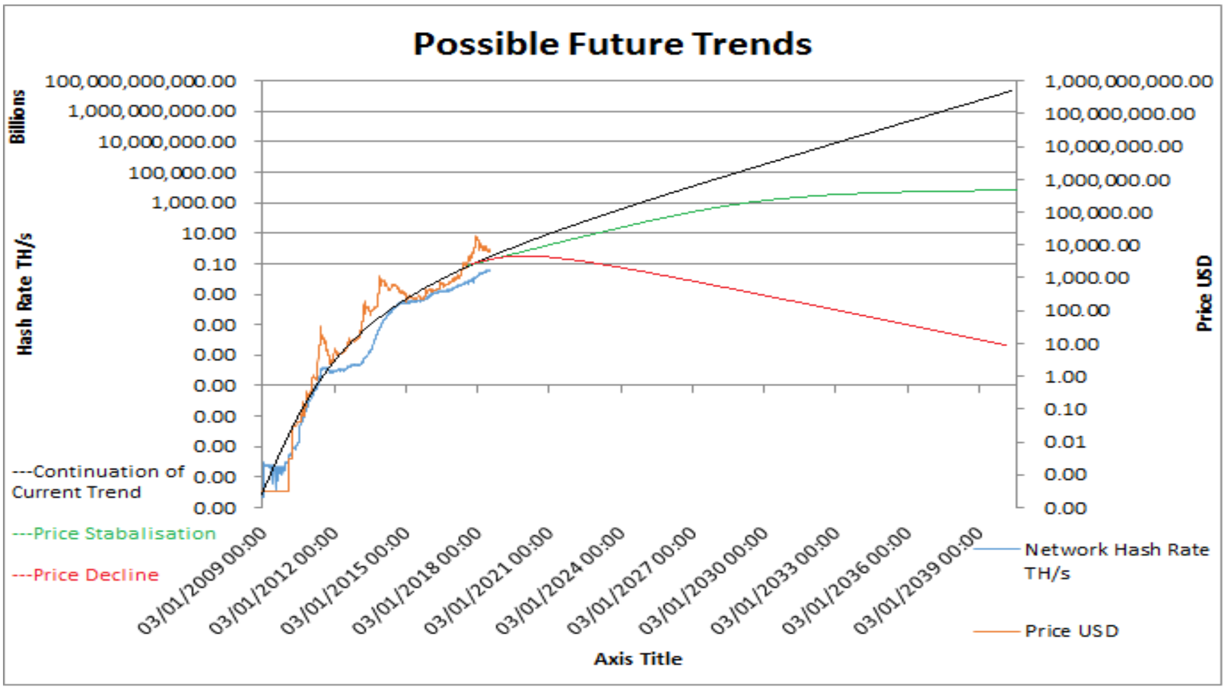


Figure 28 Three Possible Paths of Bitcoin

future energy requirements several assumptions must be made. It has been assumed that ASIC's will be the main mining equipment, and as previously identified the upper limit of their efficiency capabilities will peak in 2019.

Forecasted 2040 Energy Demand			
	Continuation of Current Trend	**Stable Growth**	**Decline**
Network Capacity MW	7,927,116,236.18	71,587.00	0
Annual Electrical Demand 2040 TWh	69,441,538,228.91	627	0
% of Global Generation	1928932%	2.59%	0%

Table 9 Models 2040 Energy Demand Forecast

Results generated from the worst-case scenario circumstance, in which the bitcoin network price and hash rate continues to increase at the current rate makes for daunting reading. While global energy generation is estimated to increase on average of 3% annually until 2040, Bitcoins energy demand has been increasing roughly 300% per annum for the past several years. Should this network expansion and price rise continue, the network would be capable of consuming 50% of global electricity generated by 2024, and require double global capacity by 2026.

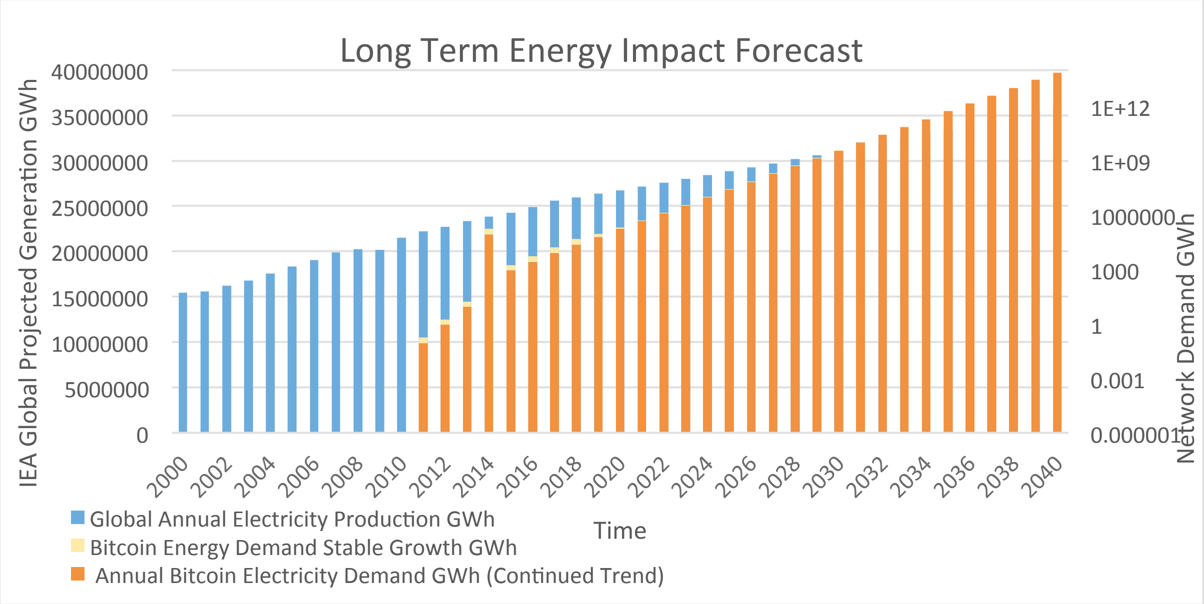


Figure29 2040 Electrical Generation forecast Compared to the Continuation of Bitcoin Network Expansion

Considering the necessity to increase generation to accommodate this rise in electrical demand, the new generation deployment required to support the network highlights the feasibility of this being realised. Nuclear alone with the greatest power density would require 2451938 km^2 or 0.005% of the earth's surface worth of new nuclear facilities, and biomass would require almost 7.9% of Earths total surface area. These figures are extreme scenarios, and it is important for them to remain in context in order to refrain from misinterpretation. While this is a continuation of the overall current trend, it is unrealistic to expect these figures to be achieved due to a number of factors such as the limitations of production by not only the energy generation sector, but the ASIC industry, and that it is reasonable to assume that technological advances will allow for alternate mining hardware of greater efficiencies that cannot be accounted for at this time or in this model. It should also be noted that in such an event that prices continue to rise at historic rates it is unlikely

Required 2040 Deployment by Area Km2					
Generation Method	**Nuclear**	**Solar PV**	**Wind Offshore**	**Wind Onshore**	**Biomass**
Average Power Density GWh/km2	3233.00	61.84	22.64	872.4	2.13
Area Required km2 Continuation of Current Trend	2451938	128187520	350137643	9086561	3721650815
Area Required km2 Stable Growth	35.3864	1850.0060	5053.1966	131.1375	53710.9726

Table 10 Area required by 2040 to support Bitcoin Network Should current Expansion Rate Continue

that electricity generators, suppliers or governments would prioritise industrial electricity demand or accommodate Bitcoin mining over domestic requirements. It can also be assumed that once the upper limits of available electricity are reached network expansion rates will decrease, suggesting that as this market matures more stabilized growth is a more plausible outcome. The stabilized growth estimations indicate by 2040 2.59% of global electricity production would be required to achieve the network hash rate and price indicated in the price stabilisation trend. This estimation may appear considerably more conservative, but when the area required to support a network of this size is considered such as 5000 km^2 of off shore wind turbines the impact appears considerably larger.

6.3. Part C - Comparison of Financial Systems

Energy Comparison of Fiat Currency Minting		
	Annual Demand TWh	**Daily Demand TWh**
Total legacy Banking System	638.89	1.75
Paper Note Printing	5.11	0.014
Coins Minting	11.00	0.030
Bitcoin	40.21	0.11

Table 11 Comparison of Fiat Currency minting to Bitcoin Minting Process

Results from the analysis of physical currency minting indicate that Bitcoin already requires more energy than global paper and coin minting processes combined. While it is less efficient in terms of currency minting the electricity demand of Bitcoin accounts for both transaction validation and coin minting, and as such when the annual demand of the entire banking system is compared it can be seen that Bitcoin on uses 1/16th of the energy required.

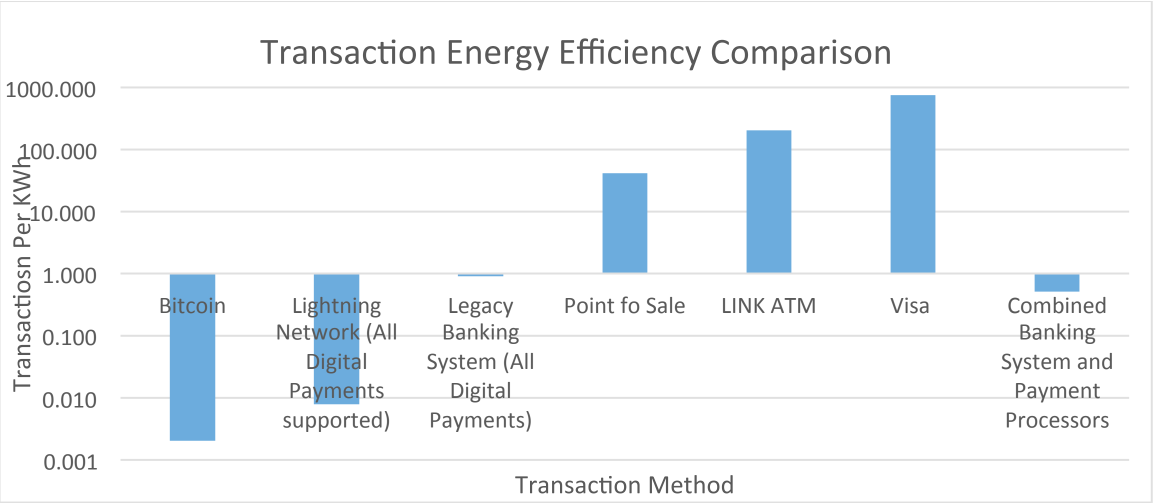


Figure 30 Transaction Efficiency Comparison

Figure 30 offers an insight into the transaction efficiency of each layer and transaction method as well as the potential impact of the Lightning Network should Bitcoin and the Lightning network become the dominant digital payment method. As can be seen Bitcoin is by far the least efficient payment method in terms of transactions per KWh. Assuming that a fully functioning Lightning Network would handle all digital payments it would increase the network efficiency considerably but still leave it less efficient than the current legacy banking system. There is little doubt from the evidence that Visa-net, LINK ATM machines or

Point of Sale devices are far more efficient in terms of transactions per KWh individually. However the analysis of these systems fails to highlight that none operate independently, and as such a better indication of how the bitcoin network compares is a cumulative comparison of the total banking system. As figure 26 shows if all digital payments are considered with the combined total electrical demand of each network the overall efficiency is reduced dramatically but still remains considerably more efficient than bitcoin or the Lightning Network. It is important again to give perspective to these results, as it reasonable to assume that Local Banks branches, ATMS and point of sales terminals would still exists and continue to play a large part in the banking and commercial sector should a crypto currency be the dominant global payment method, many of these systems would still be part of the network.

7 Conclusion

The rapid price increase of bitcoin we have witness in recent years has been a major driver in speculative investment and interest. While the price per coin has been in decline over recent months the total network hash rate has grown exponentially and subsequently its energy demand has almost doubled during this period. This network growth will likely recede in the short term if price continues to decline as mining profit margins are squeezed towards equilbirium. However should the trend reverse and the price continue to climb at previous rates, the systemic relationship with resources would cause further increase in total network hash rate and mining operations as profit margins increase once more. With out swift deployment of new generation stations to account for this growth it could have an impact on global energy markets as network energy demand outpaces supply.

Analysis indicates that daily trends in price have a minor but systematic effect on hash rate and energy demand, validating the assumptions made about rational mining based on profitability and that if price increases so will speculative interest and the network. It appears reasonable that many miners interested in profit alone change the currency they are mining on a daily basis depending on which is most profitable. Should this be true the impact on energy markets would likely be less problematic on a daily basis as these mines would already be mining continuously, drawing a steady base load from an electrical network, but highlighting the necessity for further work in estimating the entire industries electrical demand.

Findings from the analysis of mining hardware identified that decreasing transistor size in ASIC mining equipment is a driver in the increasing energy demand of the network, despite the efficiency increases of mining equipment. Due to the competitive nature of the mining process, the impact of increased hardware efficiency inevitably leads to all miners increasing the efficiency of their equipment in order to remain competitive. While it would be expected in most cases that this would reduce energy intensity of the network the opposite was found. The analysis found that while transistor size reduced, this has allowed for increasing numbers of transistors within each unit and as such the power consumption of hardware was also increasing creating an exponential growth in hash rate and energy demand. The findings from analysis of historic energy demand suggest that the progression from FPGA to ASIC had a considerable impact on reducing the network electrical demand. When the upper efficiency limits of ASIC mining equipment are reached, until an alternate transistor technology is implemented there will likely be a similar impact on the hash rate and energy demand as witnessed in 2014. Should price also increase this could create a significant rise in energy demand. The historic growth analysis highlights the impact new technology and significantly increased efficiency had on the network electrical demand, should this trend repeat itself the energy demand and pressure expect to be placed on electrical networks will be mitigated in the short term as miners upgrade their equipment.

Making future predictions of a volatile system with numerous factors and assumptions is a difficult task and as such while the findings offer an insight into the possibilities they should be viewed with caution and consideration to these facts. The tool developed works well for daily energy estimations and is a robust attempt at identifying the true electricity demand of the network thus far. While the outputs of daily metrics should be trusted, the estimations of future trends should be viewed with caution, as the model does not account for external factors or dramatic changes in technology. Short term future estimations appear reasonable and valid however the long term estimations are more challenging due to the many unknowns regarding hardware, price and hash rate progressions relying on assumptions.

The long term forecasts achieved for a continuation of the current trend highlight the limitations of the model and global electrical generation. It is unrealistic to expect the electrical demand of the network to follow previous growth rates continuously until 2040 due to the obvious pressure subsequently placed on electric supply and demand networks. However it does well to highlight the unsustainable growth we have seen previously, and indicates that should this network continue to expand stable growth is far more likely as the market matures and the marginal cost of mining reaches equilibrium.

The impact on global electricity generation by source and required deployment found some of the most interesting results. While it highlights that although current demand is large in comparison to the electrical demand of an individual or household, it is a fraction of global electricity generation, of the largest electricity generation stations, and a fraction of several nations generation capacity. This suggests the network is still far from secure from a global energy standpoint.

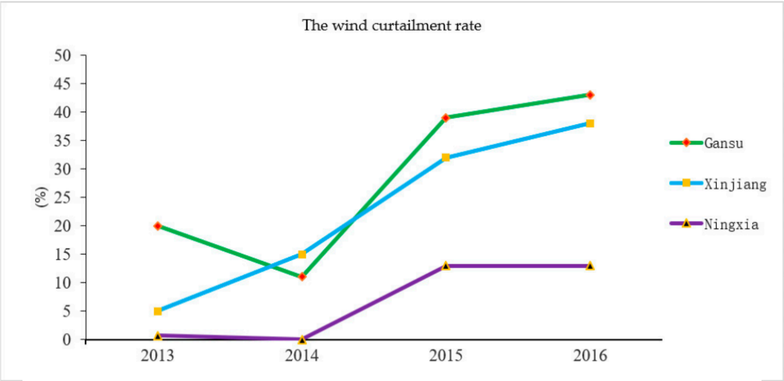


Figure 31 Wind Farm Curtailment Rates China

Research highlighted that the majority of large scale mining operations are already focused on system efficiency and on utilising renewable sources of electricity due to the low LCOE that they achieve. Considering the falling LCOE of renewable electricity generators, it is also reasonable to assume that current and future mining operations will continue to be attracted to regions with large renewable assets generating low cost energy for the industrial sector. Research found the Bitmains Oros mine has alleged daily electrical costs of $39000. At the rate of 0.04 $/KWh this would suggest an electrical capacity of 975 MW, with reports suggesting that this is supplied predominantly by coal. With high wind turbine curtailment rates in the neighbouring Gansu wind farm there appears an opportunity for mining and electrical infrastructure to create symbiotic relationships by reducing curtailment and increasing profits, and shift away from fossil fuels. [45] However the high electrical draw from the mine, reiterates the necessity for future works to apply this model to alternate PoW currencies and investigate the entire industry energy demand.

Figure 2.1 Global levelised cost of electricity from utility-scale renewable power generation technologies, 2010-2017

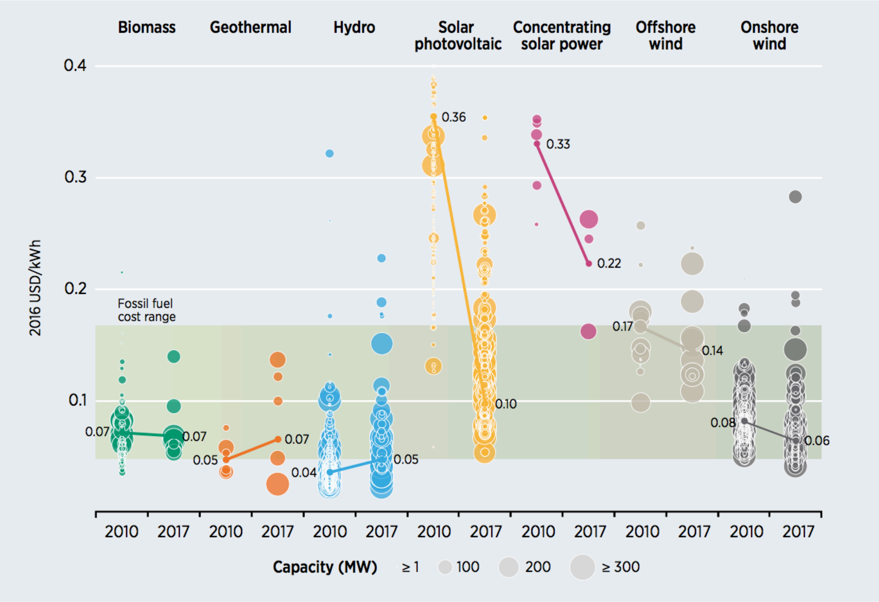


Figure 32 Average LCOE of Renewable Generation Sources, Source: Irena Renewable Source Database

Due to their dispatchable nature; hydro, nuclear, geothermal and coal are likely to be mining operations preferred generation source. Many renewables such as solar while not dispatchable offer firm power and vary with season creating further curtailment and added challenges to the balancing of energy networks. Turnkey containerised mining solutions are becoming an increasingly attractive solution for those looking for fast deployment and could offer a profitable solution to reducing curtailment of similar generation assets. [46]

Comparison of the transaction efficiency highlights the challenges yet to be overcame should Bitcoin or any other crypto currency intend on becoming the major digital currency or payment method. While far behind systems such as visa in terms of transaction volume and efficiency, it is not that far behind the entire banking system when the layers are combined, which appears as a far more accurate comparison. Should the Lightning Network proves successful, it still won't be as efficient as the legacy banking system, and as its overall energy demand is likely to increase it will only continue to become less efficient unless the volume of digital transactions increase beyond the current electrical demand growth rate.

Due to the decentralized nature of bitcoin and blockchain, the negative connotations are also amplified due to the inability to regulate the market. Bitcoin advocates argue that the security, immutability and borderless nature are worth the resource intensity of the PoW protocol, however its is also suggested that the network will have to consume 50% of global electricity generated in order to be truly secure. This is an unnerving thought from am energy and sustainability stand point and the implications of a decentralized unregulated system that generates profits in a framework of capitalism suggests that as long as its profitable, the network will continue to grow. Another implication of an unregulated economic system is the eventual centralization of such systems. The laws of Pareto distribution dictate that this is an inevitable consequence of any economic system, and it appears that this is already taking place. Should Bitmain have a 70% market share of the ASIC manufacturing industry, and several of the worlds largest mines it would not be in their interest to reveal this, as it would undermine the decentralisation of the network and ultimately their own market valuation and profitability. As the centralization of ASIC manufacturing and mining appears already underway we must ask ourselves what impact this will have on the viability of PoW consensus and global sustainability targets.

The value of bitcoin is objective and the value proposition and benefits can be debated at length. But in a decentralised lassez faire economic model, if something is profitable there are always going to be parties willing to prioritise profit over the environment or ensuring sustainability. Thus it would appear that continued rapid inflation and the subsequent profits while a great driver in adoption, are one of the biggest challenges facing decentralised currencies should they require resource intensive processes to ensure compliance. The inevitable Industrialisation of the mining process indicates that PoW mining is highly susceptible to centralisation and a Tragedy of the Commons scenario occurring should price continue to climb at historic rates.

Ultimately we must ask our selves; are the resources required to support a digital decentralised global currency using the PoW consensus mechanism worth the promises of financial inclusion, borderless payments, fiscal autonomy and fraud prevention that the network claims to provide? Bitcoin has done well to achieve a balanced eco system with miners, developers, business and end users all with differing interests ensuring no single party has complete control of the network, but with a lack of central authority reaching consensus and a shift away from PoW seems increasingly unlikely, suggesting we will likely witness further industrialization of our landscape natural, with the environment and our natural resources paying the ultimate price.

The findings suggest that the implications of this technology must be considered not only by national economic policy makers, but also by those responsible for energy policy. The resource intensive nature of this technology combined with its unregulated nature and rapid growth suggest it is only a matter of time before the challenges of its electrical demand impact electrical networks. There is large potential for this industry and it is essential policy makers develop an understanding of the implications and ensure that if crypto currency mining facilities are to be deployed within their boundaries that they work un unison and compliment current electrical generation systems rather than put further strain on them and the surrounding networks.

8. Future Works:

The main focus of this work was to develop a tool and methodology for making accurate estimations of the Bitcoin energy demand. Further work to make future estimations and compare the energy demand of current banking infrastructure were limited and have potential to be taken further. Due to the lack of knowledge on electricity sources the emissions generated by this industry where not considered due to the potential for misleading readers. Future work on estimating the geographical breakdown of mining facilities and typical generation mix of these could be a means of generating meaningful emissions data.

Through this work there are opportunities for future work to progress both parts of this comparison and develop the methodologies created further. As this industry matures the transparency of mining companies and ASIC manufacturers are likely to improve, allowing for better data sets and reduced/validated assumptions. Energy estimates of the current banking system could be improved through the acquisition of more specific data sets from all payment processors. Applying the tool and methodology developed to other PoW crypto currencies in order to make estimates of the entire industries energy demand is another possible future work that has yet been undertaken and would likely produce interesting results

9. References:

[1] Claire Provost. 2013. Why do Africans pay the most to send money home? (January 2013). http://www.theguardian.com/global-development/2013/jan/30/africans-pay-most-send-money.

[2] Rachel Banning-Lover. 2015. Boatfuls of cash: how do you get money into fragile states? (February 2015). http://www.theguardian.com/global-development-professionals-network/2015/feb/19/boatfulsof-cash-how-do-you-get-money-into-fragile-states.

[3] CGAP. 2008. Making Money Transfers Work for Microfinance Institutions. (March 2008). http://www.cgap.org/sites/default/files/CGAP-Technical-Guide-Making-Money-Transfers-Workfor-Microfinance-Institutions-A-Technical-Guide-to-Developing-and-Delivering-MoneyTransfers-Mar-2008.pdf.

[4] Asli Demirguc-Kunt, Leora Klapper, Dorothe Singer, and Peter Van Oudheusden. 2015. The Global Findex Database 2014 Measuring Financial Inclusion Around the World. Policy Research Working Paper 7255. World Bank. http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2015/04/15/090224b082dca3aa/1_0/Rendered/PDF/The0Global0Fin0ion0around0the0world.pdf.

[5] David Mazieres. (2015). *Stellar Lumen Protocol.* Available: https://www.stellar.org/papers/stellar-consensus-protocol.pdf.

[6] UK Finance. (2017). *Quarterly Market Trends.* Available: https://www.ukfinance.org.uk/wp-content/uploads/2017/11/Quarterly-Market-Trends-Q3-2017.pdf.

[7] Visa. (2018). *Visa Service Disruption.* Available: https://www.visaeurope.com/newsroom/news/visa-service-disruption. Last accessed 15/06/2018

[8] International Monetary Fund. (2018). *REPÚBLICA BOLIVARIANA DE VENEZUELA.* Available: https://www.imf.org/en/Countries/VEN#countrydata.

[9] Satoshi Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *https://bitcoin.org*. 1 (1), 1-9

[10] Corin Faife. (2017). *Bitcoin Hash Functions Explained.* Available: https://www.coindesk.com/bitcoin-hash-functions-explained/

[11] Cynthia Dwork, Moni Naor. (1993). Pricing via Processing or Combating Junk Mail. IBM Research Division, Almaden Research Centre. 1-11

[12] Adam Back. (May, 1997).Hashcash. Published at: http://www.cypherspace.org/hascash/

[13] Hal Finney. (2004). *Reusable Proof of Work.* Available: https://nakamotoinstitute.org/finney/rpow/index.html.

[14] Wouter Penard, Tim van Werkhoven.. (2005). On the Secure Hash Algorithm Family. *Encyclopedia of Crpytography and Security*. 1 (1), https://doi.org/10.1007/0-387-23483-7

[15] Tim Fisher. (2018). *Cryptographic Hash Function Use a cryptographic hash function to verify the authenticity of data.* Available: https://www.lifewire.com/cryptographic-hash-function-2625832.

[16] Julien Prat & Benjamin Walter, 2018. "An Equilibrium Model of the Market for Bitcoin Mining," CESifo Working Paper Series 6865, CESifo Group Munich. https://ideas.repec.org/p/ces/ceswps/_6865.html

[17] Marcel Thum, 2018. "The Economic Cost of Bitcoin Mining," CESifo Forum, Ifo Institute - Leibniz Institute for Economic Research at the University of Munich, vol. 19(1), pages 43-

45, March. https://www.cesifo-group.de/DocDL/CESifo-Forum-2018-1-thum-bitcoin-march.pdf

[18] Alex De Vries. (2018). Bitcoin's Growing Energy Problem. *Joule*. 2 (5), 801-805

[19] Hayes, Adam, A Cost of Production Model for Bitcoin (March 19, 2015). Available at SSRN: https://ssrn.com/abstract=2580904 or http://dx.doi.org/10.2139/ssrn.2580904

[20] Song, J. Just how profitable is Bitmain? 2017. https://medium.com/@jimmysong/just-how-profitable-is-bitmain-a9df82c761a

[21] Morgan Stanley. Bitcoin ASIC production substantiates electricity use; points to coming jump. 2018. https://ny.matrix.ms.com/eqr/article/webapp/b974be48-effb-11e7-8cdb-6e28b48ebbd3.

[22] GMO Internet. (2018). *Cryptocurrency Mining Business: Monthly Report for July 2018.* Available: https://ir.gmo.jp/en/pdf/irlibrary/disclose_info20180803_e.pdf.

[23] Marc Bevand. (2017). *Bitcoin Electricity Consumption.* Available: http://blog.zorinaq.com/bitcoin-electricity-consumption/. Last accessed 15/07/2018

[24] Giga-Watt. (2018). *What We Offer.* Available: https://giga-watt.com/.

[25] Rachel Pipan. (2018). *Bitfury CEO Announces Major Norway Expansion, Meets with Government Officials.* Available: https://bitfury.com/content/downloads/03_20_18_bitfury_norway_datacenter_release.pdf.

[26] Zheping Huang & Joon Ian Wong. (2017). *The lives of bitcoin miners digging for digital gold in Inner Mongolia.* Available: https://qz.com/1054805/what-its-like-working-at-a-sprawling-bitcoin-mine-in-inner-mongolia/.

[27] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," *25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*, Limerick, 2014, pp. 280-285. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6912770&isnumber=6912720

[28] Gordon E Moore. (1965). *Cramming More components onto Integrated Circuits.* Available: https://drive.google.com/file/d/0By83v5TWkGjvQkpBcXJKT1I1TTA/view.

[29] GMO Internet. (2018). *Worlds first 7nm Mining Chip.* Available: https://gmominer.z.com/en/.

[30] Hass McCook (2014). *A critical assessment of the Bitcoin mining industry, gold production industry, the legacy banking system, and the production of physical currency*. Available:: https://www.scribd.com/doc/228253109/The-Relative-Sustainability-of-the-Bitcoin-Network-by-Hass-McCook.

[31] Blockchain Info. (2018). *Confirmed Transactions Per ay.* Available: https://www.blockchain.com/charts/n-transactions.

[32] Capgemini. (2018). *Non Cash Payment Volume.* Available: https://www.worldpaymentsreport.com/#non-cash-payments-content.

[33] Joseph Poon, Thaddeus Dryja. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. *Lightning Network White Paper. Available: https://lightning.network/lightning-network-paper.pdf*

[34] ASIC Miner Value . (2018). *ASIC Manufacturer Directory.* Available: https://www.asicminervalue.com/manufacturers.

[35] Bitcoin Wiki. (2018). *ASIC Mining Chip List, ASIC Development Projects.* Available: https://en.bitcoin.it/wiki/List_of_Bitcoin_mining_ASICs.

[36] Blockchain Info. (2017). *Hash Rate.* Available: https://www.blockchain.com/charts/hash-rate.

[37] Blockchain Info. (2017). *Difficulty.* Available: https://www.blockchain.com/charts/difficulty.

[38] Internation Energy Agency. (2017). *Headline Energy Data.* Available: https://www.iea.org/statistics/?country=WORLD&year=2015&category=Key%20indicators&indicator=TPESbySource&mode=chart&categoryBrowse=false.

[39] Vincent K M Cheng, Geoffrey Hammond. (2014). Energy density and spatial footprints of various electrical power systems. *Energy Procedia*. 61 (1), 578-581

[40] LINK ATM. (2017). *statistics and Trends.* Available: https://www.link.co.uk/about/statistics-and-trends/.

[41] Kurt W. Roth, Fred Goldstein, Jonathan Kleinman. (2002). Energy Consumption by Office and Telecommunications Equipment in Commercial Buildings. *Energy Consumption Baseline*. 1 (1), 166-167

[42] The UK Card Association. (2018). *UK Card Payments 2017.* Available: http://www.theukcardsassociation.org.uk/wm_documents/UK%20Card%20Payments%202017%20%20website%20FINAL.pdf.

[43] Verifone. (2018). *Verifone POS Terminal Specifications.* Available: https://www.wirelessterminalsolutions.co.uk/product/verifone-vx670-verifone-vx680-standard-charging-base/.

[44] Visa. (2018). *Visa Corporate Responsibility Report.* Available: https://usa.visa.com/dam/VCOM/download/corporate-responsibility/visa-2016-corporate-responsibility-report.pdf.

[45] Guoliang Luo, Erli Dan, Xiaochun Zhang, Yiwei Guo. (2018). Why the Wind Curtailment of Northwest China Remains High. *Sustainability*. Available: www.mdpi.com/2071-1050/10/2/570/pdf

[46] Bitfury. (2018). *Black Box.* Available: https://bitfury.com/hardware/blockbox.

10 Appendices

Appendix A…………..………ASIC Hardware Statistics…………….…………EXCEL Tab 1

Appendix B…………………Profitability Table……………………………….EXCEL Tab 2

Appendix C…………………Network Hardware Breakdown………..………EXCEL Tab 3