Bitcoin Resource: Anonymity & Challenges

North South University

Department of Electrical & Computer Engineering

Instructor's Name: Mohammad Ashrafuzzaman Khan

Course - CSE499A

Section -10

Group -2

Submit: 23rd December 2019

Md. Ikbal Hossain	1510786042
Ibrahim Khalil	1520775042
Abul Kawsar	1531500042
Md. Faisal Hossan Shakib	1521156642

Abstract

In this article we tried to show how bitcoin network is working despite the fact of its anonymity. We found about a fixed number of total bitcoins which was mentioned as resource of bitcoin. But we don't know if it is really existing or any equivalent resource to bitcoin is available or not. Thus, we can say the network system could be based on a hype where the system is still working effectively. And there is one challenging thing that, those who mine bitcoin need to solve algorithm related problems, and for that very high configuration PC is required. For this, it seems from normal computer it may not be possible to mine bitcoin or it could damage the PC if it is attempted.

Table of Contents

List of Figures

List of Tables

1. **Introduction**

Bitcoin is a cryptocurrency that is known as a digital asset planned to function as an exchange medium that uses powerful cryptography to secure monetary transactions, monitor the development of extra units, and verify asset transfer or exchange. It is an online virtual currency which is already being used based on public key cryptography, proposed in 2008 in a paper [1] written by someone named Satoshi Nakamoto as pseudonym. It is fully working from January 2009 and its broad acceptance, simplified by the presence of exchange markets allowing easy changing with conventional currencies (EUR or USD), has brought it to be the most useful digital currency.

Satoshi Nakamoto, regarded as the founder of bitcoin, addressed the reliance of the internet on trustworthy third parties such as banks and credit card companies to process digital payments. The traditional method is still working for most transactions around the world but problems may occur when financial institutions simply the buying and selling of goods on the internet. The standard method is used to recognize as unavoidable a definitive degree of fraud. Yet fraud raises the cost of doing business more or less for everyone. Nakamoto suggested this digital payment system based instead of trust on cryptographic evidence.

2. Background

Bitcoin, was first released as an open-source software in 2009, it is generally considered as the first decentralized cryptocurrency. After the release of it, more than 6,000 altcoins have been established.It is used anywhere in the world to safely store and move any quantity of a third party's inte rest.It is a distributed decentralized currency without a central bank or single administration that can be sent without any intermediaries to peer bitcoin network. Over the course of bitcoin's history, it has undergone rapid growth to become a significant currency both on and offline from the mid2010.

2.1 Fiat currency and Bitcoin

Fiat currency is a money that is issued /printed by government and has a legal tender. The U.S. dollar is fiat money, as are the Euro, BDT and many other major world currencies. In some countries bitcoin is not fiat money like other currencies.[6]

2.1.1 Fiat currency vs Cryptocurrency

There are two types of currencies either its fiat or cryptocurrency.

Fiat is "legal tender" backed by a "central government." It can take the form of physical dollars or it can be represented electronically, such as with bank credit. The government controls the supply and you can use fiat to pay your taxes.

Cryptocurrency is not backed by a central government or bank as it is decentralized and global. Its form is more like bank credit sans the bank. An algorithm controls the supply and you can't pay your taxes with it.

The most significance difference between fiat and cryptocurrency is that they both operates in a different way. With bitcoin the transition happens quickly and without involving of a third party but with an online fiat money exchange a some of e-money(USD,BDT,EURO ETC) is translated into an equal amount of e-value through the use of mobile wallet. [6]

2.1.2 Is Bitcoin a Fiat Currency?

As stated earlier, a fiat currency is a money that is not backed by gold or any other hard asset. Its value is declared by fiat alone – the issuing government simply decrees that the currency has worth. You can't trade a Bitcoin for an ounce of gold at a fixed price. Cryptocurrency isn't issued by any government and there's a fixed ceiling on how many can exist.[6]

2.1.3 Why Bitcoins have values?

Bitcoin provides an effective way to transfer money over the internet and is operated by a decentralized network with a straightforward set of rules that offer an alternative to fiat money controlled by central banks. Bitcoin and other digital currencies have been touted as alternatives to fiat money. [3]

But what gives any type of currency value?

Answer: Because it is exchangeable easily and we know that the thing which can be exchangeable has values.[3]

2.1.4 Why Bitcoin values changes so much?

- Like all products that have a finite supply, a bitcoin's value is determined from the numb er of people who want to buy it vs the number of people who want to sell it.
- If more people want to buy bitcoins than are currently for sale (for example if a surge of people want to start using bitcoins to transfer value across borders, see more on this below) then the price goes up.
- If more people wants to sell bitcoins than currently who wants to buy them, then the price goes down.
- One of the reasons that the price of bitcoin is so volatile is that many of the people buying bitcoins today are buying based on speculation(Speculation refers to the act of conducting a financial transaction that has substantial risk of losing value but also holds the expectation of a significant gain.) not because they actually want to use them.

Speculative buyers believe that in the future many people will want bitcoins (if this is true these future buyers will drive the price up) so speculators buy bitcoins now in anticipation of that future demand and price increase. However, speculative buyers are very sensitive to current events - news stories can quickly

turn speculative buyers into speculative sellers. This flip-flopping of speculator sentiment is the main reason the price of bitcoin varies so wildly.[3]

2.2 BITCOIN IS LIKE GOLD!

Bitcoin's Perceived Value Sways.

(i) The perceived value store versus the fiat currency is one reason why Bitcoin may fluctua te against fiat currencies. Bitcoin's properties make it gold-like. It is monitored by a design decision by the developers of the core technology to limit its production to a fixed amount, 21M BTC. [7]

(ii) Since this differs significantly from fiat currency controlled by governments that want to maintain low inflation, high employment, and adequate growth through investment in c apital resources, as fiat currency economies show signs of strength or weakness, shareh olders may allocate more or less of their resources to Bitcoin.[7]

2.3 Prototype of Bitcoin

Let us find out how the whole bitcoin thing works.

2.3.1 How Bitcoin mining works?

According to our research we found that there is a fixed 21million bitcoin set up by the core developers. When Bitcoin miner's does mining (solves algorithms) they get rewards as Bitcoin from the core developers. So basically, we can see that the miners share their resources to solve algorithms and for the rewards they get bitcoins from the core developers. Then the miners store it to the bitcoin wallet to sell it or exchange it. The more people joins the bitcoin network the more difficult the algorithms become to solve. So the Miners uses a pool method to solve the problem.[4]

Miners: Who uses resources to solve Algorithms/math problems by using special kind of software (CGMiner, Multiminer , BitMiner etc.).[4]

Resources: At beginning the mining is usually happened by just using normal computer. But it used lots of power then they used GPU's which was able to solve the problem faster but it was also power consuming too then a special kind of chip is made which is called ASIC.It uses less power and works faster.

Pool Method: A group of miners who share their resources within the group to solve more difficult algorithms then they share their rewards among them.[4]

2.3.2 How to Store Bitcoin: Cold storage is an offline wallet provided for storing bitcoins. With cold storage, the digital wallet is stored on a platform that is not connected to the internet, thereby, protecting the wallet from unauthorized access, cyber hacks, and other vulnerabilities that a system connected to the internet is susceptible to.[4]

2.3.3 Where does the math problem comes from?

- It was given by the core developers (As per our findings)!
- The more people joins the bitcoin network the more difficult the algorithms become to solve
- So the Miners uses a pool method to solve the problem.

2.3.4 What is the Resources of Bitcoin?

As per our initial finding we can say that the resource of our bitcoin is 21million BTC. Which is a fixed amount set up by the core developers who developed the bitcoin.

At first, we can say that its like gold .How?

The more people joins the network it becomes more difficult to solve the algorithms. So when they solves the algorithms they get rewards as bitcoin(gold).So more people joins in the mining, it becomes more difficult to earn bitcoin because it has a fixed amount of value as like gold ,we know that there is a fixed amount of gold in earth which is approximate of 171,300 tones (BBC).So bitcoin is like same there is fixed amount of it when more people joins to mining the more it becomes difficult to get.

3. **Methodology**

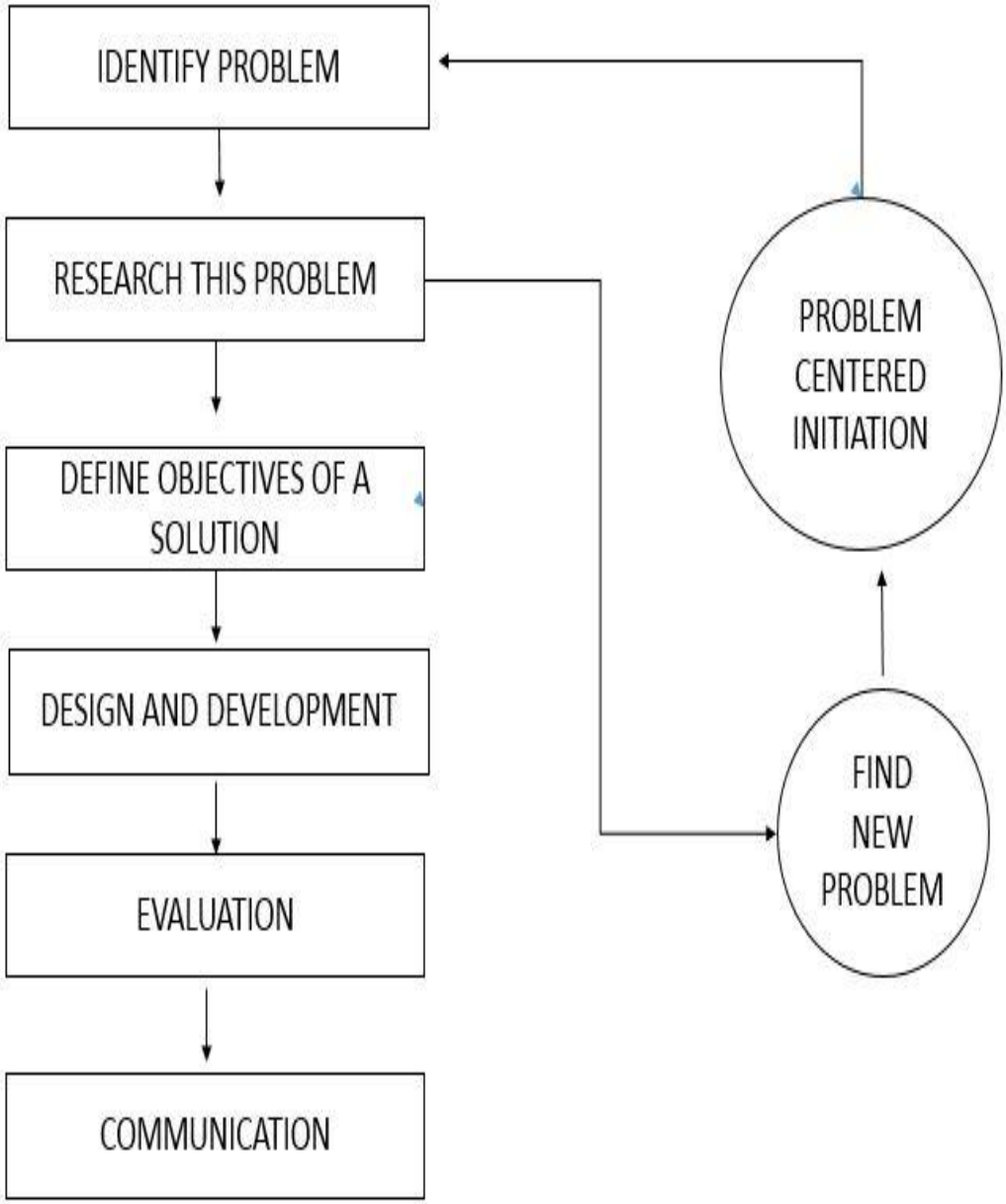

Fig. 1 Flowchart of work progress

WEEK	OUTPUT
1ST WEEK TO 3RD WEEK	TOPIC SELECT
4TH WEEK	IDENTIFY PROBLEM
5TH WEEK	RESEARCH THIS PROBLEM
6TH WEEK	NEW PROBLEM IDENTIFY
7TH WEEK	MIDTREM PRESENTATION
8TH & 9TH WEEK	SOLVE SOME PROBLEM
10TH WEEK	FINAL PRESENTATION

Table- 1 Methodology table of work progress

4. Results and Discussion

Alex de Vries, a bitcoin specialist at PwC, estimates that the current global power consumption for the servers that run bitcoin's software is a minimum of 2.55 gigawatts (GW), which amounts to energy consumption of 22 terawatt-hours (TWh) per year—almost the same as Ireland

Currently, the tool estimates that **Bitcoin** is using around seven gigawatts of **electricity**, equal to 0.21% of the world's supply. That is as much **power** as would be generated by seven Dungeness nuclear **power** plants at once.

Bitcoin mining profit depend on four parts-Hash rate, Bitcoin price, Power consumption(watts), Cost per kw/h$.Hash rate, Bitcoin Price increase and Power consumption, cost per kw/h decrease then get profit.

What is hash Rate

The **hash rate**, is a measure of how many times the network can attempt to complete this puzzle every second. This means that **hash rate** is a good indicator of the **Bitcoin** network's health

ASIC models

Search:

Model	Release	Hashrate	Power	Noise	Algo	Profitability
Innosilicon G32-1800	Nov 2019	328 GPS	1800 W	76 db	2	$117.79 /day
Innosilicon G32-500	Jan 2020	100 GPS	520 W	75 db	2	$35.99 /day
Innosilicon G32-Mini	Nov 2019	21.5 GPS	140 W	65 db	2	$7.66 /day
Bitmain Antminer S17+ (73Th)	Dec 2019	73 Th/s	2920 W	75 db	SHA-256	$2.54 /day
FusionSilicon X1 Miner	Jan 2019	12.96 Gh/s	1110 W	72 db	Lyra2REv2	$2.52 /day
Innosilicon A10 ETHMaster (500Mh)	Sep 2019	500 Mh/s	750 W	75 db	EtHash	$2.39 /day
Innosilicon A10 ETHMaster (485Mh)	Sep 2018	485 Mh/s	850 W	75 db	EtHash	$1.97 /day
Bitmain Antminer S17 Pro (53Th)	Apr 2019	53 Th/s	2094 W	82 db	SHA-256	$1.92 /day
StrongU STU-U6	Nov 2019	440 Gh/s	2200 W	76 db	X11	$1.83 /day
Bitmain Antminer S17 Pro (50Th)	Apr 2019	50 Th/s	1975 W	82 db	SHA-256	$1.81 /day

Fig- 2 ASIC available models

If we use only one Nvdia Gforce 2080ti GPU then if we want to profit then price of bitcoin should be 700 million.

Fig- 3 Profit calculator for Nvdia Gforce 2080ti

For ASIC(Bitmain Antminer S17+ (73Th)) algorithm SHA-256

Fig- 4 Profit calculator for ASIC(Bitmain Antminer S17+ (73Th)) algorithm SHA-256

ASIC price and detail

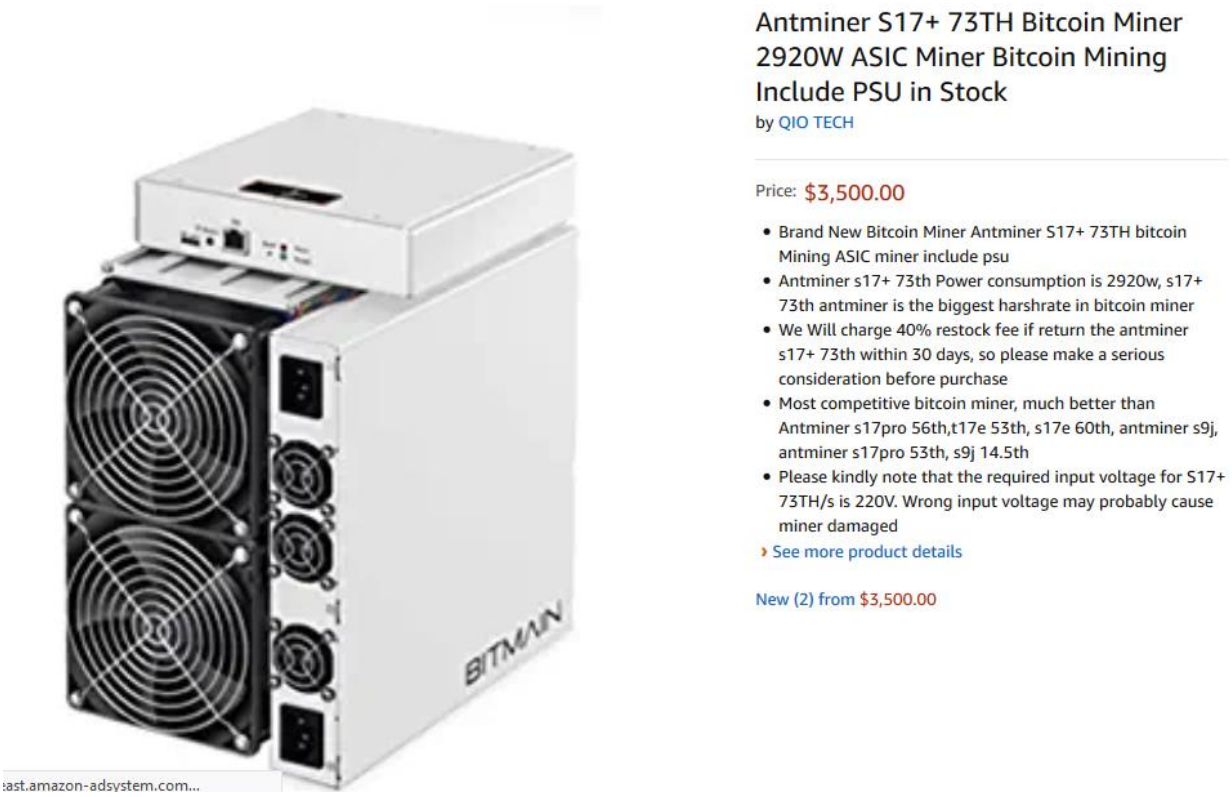

Fig-5 ASIC price and details from amazon

Gforce 2080ti price 1280$ in amazon

Fig-6 Gforce 2080ti

How much electricity does it take to mine one Bitcoin?

= If you run an Antminer 24/7 for a year it will produce about 0.85 bitcoins, at a cost of about 15000 kilowatt hours. Depending on power prices it will cost anywhere from $600 (at 3 cents per Kwh) to mine one bitcoin.

How much can you mine Bitcoin in a day?

=144 blocks per day are mined on average, and there are 12.5 bitcoins per block.144*12.5=1800.

How much does it cost to mine 1 Bitcoin?

=In USA the average cost of single Bitcoin to mine is around $4758. Rate of Bitcoin till date $7858.profit is around $3100.

What is the Fastest Bitcoin miner?

= ASIC(Bitmain Antminer S17+ (73Th)) algorithm SHA-256 has the highest hash rate of 73th per second with the energy consumption of 2920w.

How many Bitcoin are left to mine?

= There are 2,887,462.5 bitcoins left to be mined.

How Many Bitcoins Are There Now in Circulation?

= There are currently 18,112,537.5 bitcoins in existence. This number changes about every 10 minutes when new blocks are mined. Right now, each new block adds 12.5 bitcoins into circulation.

How Many Bitcoins Have Been Mined Already?

=Since bitcoins can only be created by being mined, all the bitcoins in existence are all bitcoins that have been mined. The total is 18,112,537.5 BTC.

How Many Bitcoin Blocks Are There Today?

=There have been 609,003 blocks mined.

How Many Bitcoin Have Been Stolen?

=It's unclear exactly how many bitcoins have been stolen.850,000 BTC were stolen in the Mt. Gox hack, which was the largest Bitcoin hack ever. Another 120,000 BTC were stolen from Bitfinex in 2016. Together, that adds up to about 970,000 BTC.Stolen BTC, however, does mean lost BTC. It's likely these stolen coins are still circulating, and may not even be in the hands of the original thieves.

What Happens When All 21 Million Bitcoins Are Mined?

=Right now, miners earn most of their income via the block reward. When all 21 million bitcoins are mined, there won't be a block reward to pay to miners.When a Bitcoin user sends a BTC transaction, a small fee is attached. These fees go to miners and this is what will be used to pay miners instead of the block reward.

Which software is best for Bitcoin mining?

- BTCMiner is an open SourceBitcoin Miner for ZTEX USB-FPGA modules 1.5.
- CGMiner is arguably the most famous and commonly used among Bitcoin miners at the moment.
- BFGminer is more or less the same as CGMiner.
- EasyMiner is GUI based and it acts as a convenient wrapper for CGMiner and BFGMiner software.

Smallest unit of Bitcoin?

=1 Bitcoin is Equal to 100 million Satoshis.

How much power will produce if 1000 pc are merged?

= let's assume each has core i7 3.40 GHz,500w power supply, cost of electricity 0.063$(in BD)

Total output= 3.40 GHz * 1000 (pc) = 3400 GHz = 3.4 THz

Power Consumption = 500w(Each power supply) * 1000(pc) = 500000watt=0.5 megawatt=500kw

ASIC Power consumption?

=1 ASIC chip can produce 73THz and consume 2980watt

Criteria	**1000 PC**	**ASIC**
1.Output	3.4 THz	73 THz
2.Power Consumption	0.5 megawatt	2920watt
3.Heat generated	Very High	Comparatively low
4.Cost	Very High	Comparatively very low

Table – 2: 1000 Personal Computer vs ASIC

If we use 1000 PC for bitcoin mining it is possible to mine coins but there will be no profit in fact can be in loss.

5.Conclusions and Recommendations

It's possible to mine bitcoin merging many computers but it is very costly. It's better to use ASIC for mining. 21 million can be bluff. If exist then some questions are yet to come

- What happened when the 21 million is finished?
- After mining the 21 million of bitcoin what will be the rate of bitcoin then?
- Is there any chance to control it by the government and make it legalize to prevent money stealing?
- Can anyone be a billionaire by bitcoin mining?
- How much bitcoin has Satoshi Nakamoto have and how rich he is?
- If entire people are starting bitcoin instead of dollar/taka then what will be the situation/circumstances
- Can we use bitcoin for mutual transaction instead of dollar?
- Do legal cashless currencies follow the same rule of bitcoin?
- Are there any differences if we use bitcoin for legal transections?
- How difficult are the mining math problems are?
- Many people is predicting that cryptocurrency are the future then what will happen when we will not store our money in banks and not giving taxes?

6. Acknowledgements

We would like to take this opportunity to express our profound gratitude and deep regard to our honorable faculty **Dr. Mohammad Ashrafuzzaman Khan** (Assistant Professor in Electrical and Computer Engineering (ECE) Department in North South University) for the chance to do this project. We would also like to thank him for exemplary guidance, valuable feedback and constant encouragement throughout the project. His valuable suggestions were of immense help throughout our research work. His perceptive criticism kept us working to make this project in a much better way. Working under him was an extremely knowledgeable experience for us.

We are also grateful to our group mates for their support and hard work throughout this report.

7 References

1. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. (2008)
2. Bitcoin
3. https://www.investopedia.com/articles/investing/052014/why-bitcoins-value-so-volatile.asp
4. https://www.investopedia.com/tech/how-does-bitcoin-mining-work/
5. https://www.investopedia.com/ask/answers/100314/why-do-bitcoins-have-value.asp
6. https://eaglesinvestors.com/investment-education/crypto-education/bitcoin-vs-fiat-currencies-vs-blockchain/
7. https://www.vice.com/gr/article/gqw7xx/why-bitcoins-are-just-like-gold
8. https://www.cryptocompare.com/mining/calculator/btc?HashingPower=40&HashingUnit=TH%2Fs&PowerConsumption=1500&CostPerkWh=0.12&MiningPoolFee=1
9. https://www.buybitcoinworldwide.com/mining/calculator/
10. https://whattomine.com/coins?utf8=%E2%9C%93&adapt_q_380=1&adapt_q_fury=1&adapt_q_470=1&adapt_q_480=3&adapt_q_570=1&adapt_q_580=1&adapt_q_vega56=1&adapt_q_vega64=1&adapt_q_vii=1&adapt_q_1050Ti=1000&adapt_q_10606=1&adapt_q_1070=0&adapt_q_1070Ti=0&adapt_q_1080=0&adapt_q_1080Ti=1&adapt_q_1660=0&adapt_q_1660Ti=0&adapt_q_2060=0&adapt_q_2070=0&adapt_q_2080=0&adapt_q_2080Ti=100&eth=true&factor%5Beth_hr%5D=5250.00&factor%5Beth_p%5D=22000.00&zh=true&factor%5Bzh_hr%5D=10000.00&factor%5Bzh_p%5D=22000.00&cnh=true&factor%5Bcnh_hr%5D=145000.00&factor%5Bcnh_p%5D=16000.00&cng=true&factor%5Bcng_hr%5D=310000.00&factor%5Bcng_p%5D=22000.00&cnr=true&factor%5Bcnr_hr%5D=100000.00&factor%5Bcnr_p%5D=19000.00&cnf=true&factor%5Bcnf_hr%5D=230000.00&factor%5Bcnf_p%5D=16000.00&eqa=true&factor%5Beqa_hr%5D=37500.00&factor%5Beqa_p%5D=22000.00&cc=true&factor%5Bcc_hr%5D=1080.00&factor%5Bcc_p%5D=22000.00&cr29=true&factor%5Bcr29_hr%5D=1200.00&factor%5Bcr29_p%5D=22000.00&ct31=true&factor%5Bct31_hr%5D=200.00&factor%5Bct31_p%5D=22000.00&eqb=true&factor%5Beqb_hr%5D=7300.00&factor%5Beqb_p%5D=22000.00&rmx=true&factor%5Brmx_hr%5D=138000.00&factor%5Brmx_p%5D=19000.00&ns=true&factor%5Bns_hr%5D=280000.00&factor%5Bns_p%5D=22000.00&tt10=true&factor%5Btt10_hr%5D=6000.00&factor%5Btt10_p%5D=22000.00&x1

6r=true&factor%5Bx16r_hr%5D=4100.00&factor%5Bx16r_p%5D=22000.00&phi2=true&factor%5Bphi2_hr%5D=1470.00&factor%5Bphi2_p%5D=22000.00&xn=true&factor%5Bxn_hr%5D=1010.00&factor%5Bxn_p%5D=22000.00&eqz=true&factor%5Beqz_hr%5D=5650.00&factor%5Beqz_p%5D=22000.00&zlh=true&factor%5Bzlh_hr%5D=7200.00&factor%5Bzlh_p%5D=22000.00&ppw=true&factor%5Bppw_hr%5D=3120.00&factor%5Bppw_p%5D=22000.00&x25x=true&factor%5Bx25x_hr%5D=790.00&factor%5Bx25x_p%5D=22000.00&mtp=true&factor%5Bmtp_hr%5D=460.00&factor%5Bmtp_p%5D=22000.00&lrev3=true&factor%5Blrev3_hr%5D=9850.00&factor%5Blrev3_p%5D=22000.00&factor%5Bcost%5D=0.1&sort=Profitability24&volume=0&revenue=24h&factor%5Bexchanges%5D%5B%5D=&factor%5Bexchanges%5D%5B%5D=binance&factor%5Bexchanges%5D%5B%5D=bitfinex&factor%5Bexchanges%5D%5B%5D=bitforex&factor%5Bexchanges%5D%5B%5D=bittrex&factor%5Bexchanges%5D%5B%5D=dove&factor%5Bexchanges%5D%5B%5D=exmo&factor%5Bexchanges%5D%5B%5D=gate&factor%5Bexchanges%5D%5B%5D=graviex&factor%5Bexchanges%5D%5B%5D=hitbtc&factor%5Bexchanges%5D%5B%5D=hotbit&factor%5Bexchanges%5D%5B%5D=ogre&factor%5Bexchanges%5D%5B%5D=poloniex&factor%5Bexchanges%5D%5B%5D=stex&dataset=&commit=Calculate

11. https://coinguides.org/hashpower-converter-calculator/