Department of Electrical and Computer Engineering
North South University

Senior Design Project

# Bitcoin Resource: Anonymity & Challenges

| | |
|---|---|
| Name: Md. Ikbal Hossain | #ID 1510786042 |
| Name: Md. Faisal Hossan Shakib | #ID 1521156042 |
| Name: Ibrahim Khalil | #ID 1520775042 |
| Name: Abul Kawsar | #ID 1531500042 |

Faculty Advisor:

Dr. Mohammad Ashrafuzzaman Khan

Assistant Professor

Department of ECE

Spring 2020

# LETTER OF TRANSMITTAL

April, 2020

To

Dr. Mohammad Rezaul Bari

Associate Professor and Chairman,

Department of Electrical and Computer Engineering,

North South University, Dhaka.

**Subject:** Submission of Capstone Project on “Bitcoin Resource: Anonymity & Challenges”.

Dear Sir,

With due respect, we would like to submit our **Capstone Project Report** on “Bitcoin Resource: Anonymity & Challenges” as a part of our BSc program. In The report we tried to show how bitcoin network is working despite the fact of its anonymity. And we have tried to configure whether the resource is existing or not in real. It may assist in future when currency will be mostly dependent on cryptocurrency. We tried our level best to make the report meaningful and informative.

The Capstone project was very much valuable to us as it helped us to gain experience from practical field. It was a great learning experience for us. We tried to the maximum competence to meet all the dimensions required from this report.

We will be highly obliged if you are kind enough to receive this report and provide your valuable judgment. It would be our immense pleasure if you find this report useful and informative to have an apparent perspective on the issue.

Sincerely Yours,

.........................................................

Ibrahim Khalil

Department of ECE

North South University, Bangladesh

........................................................

Md. Ikbal Hossain

Department of ECE

North South University, Bangladesh

........................................................

Md. Faisal Hossan Shakib
Department of ECE
North South University, Bangladesh

........................................................

Abul Kawsar
Department of ECE
North South University, Bangladesh

# APPROVAL

This Research Report is prepared to fulfill the requirements of our Directed Research and we (Md. Ikbal Hossain, Md. Faisal Hossan Shakib, Ibrahim Khalil, Abul Kawsar) are glad and blessed to complete this project within given time and submitting the report. We conducted this project with sheer encouragement and support from our faculty supervisor. We believe that with him beside us, accomplishment of this project seemed much easier.

The sole purpose of this report is for the course CSE 499B, which requires multidisciplinary students working together Electrical and Computer Engineering Department of North South University.to complete a research.

Hence, this is our earnest request to the respected Chairman, Department of Electrical and Computer Engineering to accept this report as the fulfillment of the degree of Bachelor of Science in Computer Science under

***Approval given by:***

………………………………

Project Supervisor  
Dr. Mohammad Ashrafuzzaman Khan  
Assistant Professor, ECE Department  
North South University  
Dhaka, Bangladesh

…………………………………

Department Chair:  
Dr. Mohammad Rezaul Bari  
Associate Professor& Chair, ECE Department  
North South University  
Dhaka, Bangladesh

# DECLARATION

This is our truthful declaration that the “**Capstone Project Report” we have prepared** is not a copy of any **“Capstone Project Report”** previously made by any other team. We also express our honest confirmation in support of the fact that the said **“Capstone Project Report”** has neither been used before to fulfill any other course related purpose nor it will be submitted to any other team or authority in future.

.........................................................

Ibrahim Khalil
Department of ECE
North South University, Bangladesh

.........................................................

Md. Ikbal Hossain
Department of ECE
North South University, Bangladesh

.........................................................

Md. Faisal Hossan Shakib
Department of ECE
North South University, Bangladesh

.........................................................

Abul Kawsar
Department of ECE
North South University, Bangladesh

# ACKNOWLEDGEMENT

First of all, we wish to express our gratitude to the Almighty for giving us the strength to perform our responsibilities and complete the report. This report is made possible through the help and support from everyone including teachers and friends. 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 report. 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 report 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.

# ABSTRACT

Different types of cryptocurrency and their transaction technologies are getting popularity among the people and various groups. In this paper 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. In this work, initially we have conducted query on two things. One is its anonymity and the other one is about the possibility of mining bitcoin in general PC.  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. Moreover, further investigation may uncover new ways to explore in this field.

## CONTENTS

# CHAPTER 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.

## CHAPTER 2: LITERATURE REVIEW

While working on this research project, we studied various research papers related to our project topic and picked a few papers from there which were conducted on bitcoin features and utilizing. We chose these particular papers because their working approach is closely related to our research work. We also deduced some ideas from there for doing our work.

## CHAPTER 2.1: EXISTING LITERATURE EXPLANATION

In this paper **Christian Decker and Roger Wattenhofer**[2] studied how Bitcoin utilizes a multi-bounce communicate to spread exchanges and blocks through the system to update the record copies. They utilize the assembled data to check the idea that the engendering delay in the system is the essential reason for blockchain forks. They suggested that Blockchain forks ought to be kept away from as they are symptomatic for irregularities among the imitations in the network. They also proposed a few changes to the present convention that, while not an answer for the inherent issues of the correspondence model utilized by Bitcoin, may alleviate them. And they presented a model that clarifies the presence of blockchain forks, and certify the model by coordinating it to their observations. They made some changes in the networks and their estimations showed that a single node actualizing these progressions decreases the quantity of blockchain forks in the system by over 50%.

**Andrew et al.[**3] proposed an adjustment to Bitcoin that repurposes its mining assets to accomplish an all the more comprehensively helpful objective. Here they named their new scheme as permacoin, a modification to bitcoin. They allude to the essential unit of mining work in Bitcoin as a scratch-off puzzle (SOP). At the time of composing, mining a Bitcoin block (bunch of coins) requires around 255 hash calculations and the Bitcoin arrange mines a block generally at regular intervals, and subsequently devours huge figuring assets and characteristic assets, for example, power, inciting boundless worry about waste. Their approach has been to supplant the fundamental computational SOP in Bitcoin with one dependent on Proofs-of-Retrievability. Given the size of the current Bitcoin organize, they gauge that their plan would reuse enough assets to store at any rate a "Library of Congress" worth of information (i.e., 200 terabytes) in an internationally circulated system.

**Dorit Ron** and **Adi Shamir**[4] discussed the answer for an assortment of inquiries regarding the conduct of the clients, how they get and how they spend their bitcoins, the equalization of bitcoins they keep in their records, and how they move bitcoins between their different records apropos to more likely secure their privacy. The authors tried to answer some precise questions like what number of various clients are there in the system? What number of bitcoins are commonly kept in each record, and how does this equalization shift after some time? Are most bitcoins kept by a couple of enormous clients? Do they keep their bitcoins in saving accounts" or do they spend them right away? What number of clients had enormous adjusts sooner or later in time? What is the size circulation of bitcoin exchanges, and what number of them are micropayments? They noticed that the subgraph which contains the huge exchanges alongside their neighborhood has numerous peculiar looking structures which could be an endeavor to disguise the presence and connection between these exchanges, yet such an endeavor can be thwarted by following the cash trail in a sufficiently diligent manner.

The aim of this paper is to understand the diffuse system of Bitcoin's prize structure and its impact over a different, decentralized populace of individual members. **Andrew et al.**[5] and his team discussed that the amplitude of mining coalition is because of a restriction of the Bitcoin proof of-work perplex – explicitly, that it bears a powerful system for authorizing participation in an alliance. They presented a few definitions and developments for "nonoutsourceable" puzzles that defeat such implementation components, along these lines dissuading alliances. To guarantee security the most central suspicion made by decentralized cryptographic forms of money is that no single substance or administration employs an enormous part of the computational assets in the orgnaisation.

It does not bring in new parties or change the security model. In this paper they portray Zerocoin, a circulated e-money system. Breaking this assumption can be cause for a massive problem in the security properties of this network. They have contributed two developments: a feeble nonoutsourceable puzzle provable in the irregular oracle model, and a nonexclusive change from any powerless nonoutsourceable puzzle to a solid one. They suggest that this could be utilized to ensure that participation as a free individual is the best mining procedure.

This paper proposed an answer for the blockchain agreement issue that doesn't require mining by adjusting a current answer for the Byzantine Generals Problem. The goal of cryptocurrency conventions, for example, Bitcoin is to keep up a live decentralized exchange record while guarding against double spend attacks from vindictive Byzantine actors that go astray from the convention. Consensus of the Bitcoin exchange record is verified by a system of miners who vie for remunerations in the blockchain. The author's commitment here is a novel consensus convention that requires no proof of-work mining and has a significant level of security against double spend attacks. And **Jae Kwon[**6] made a powerless presumption about the member's abilities to keep time, and they assume incomplete synchrony of the system.

While Bitcoin offers the potential for new sorts of budgetary association, it has huge impediments with respect to privacy. In this paper **Ian Miers et al**.[7] proposed Zerocoin, a cryptographic augmentation to Bitcoin that increases the convention to take into account completely mysterious money exchanges and their system uses standard cryptographic assumption and system that utilizations cryptographic methods to break the connection between individual Bitcoin exchanges without including confided in parties. They conclude that their works has a several open problem and further research on their works could prompt various tradeoffs between security, responsibility, and anonymity.

This paper says that if Bitcoin turns into the common installment system on the Internet, wrongdoing warriors will unite with controllers and uphold boycotting of exchange prefixes at the gatherings who offer genuine items and administrations in return for bitcoin. Here **Malte et al**[8] and the other authors designed a risk model on basis of prediction using public knowledge and data and also discussed the implications as a unit of account in the market. The ubiquity of Bitcoin among crooks, supposedly for its anonymity and free to missing guideline, has called for new ways to deal with battling money related crime submitted in or settled through Bitcoin. They proposed a promising technique that is to blacklist exchange prefixes to refute resources beginning from criminal continues. This paper considers the future of Bitcoin where boycotting of realized awful exchange prefixes is regular practice and the subsequent boycotts are seen by every pertinent parties where bitcoins can be spent.

This paper states that Bitcoin makes various bogus cases, including: tackling the double spending issue is something to be thankful for; bitcoin can be a hold cash for banking; storing rises to sparing; and that we ought to accept bitcoin can extend by emptying to turn into a worldwide transactional money supply. Bitcoin is a computerized money begun in 2009 that makes one of a kind, non-duplicable electronic tokens utilizing programming (dubbed mining) with an asymptotic breaking point of formation of 21 million tokens. At regular intervals of four years, the quantity of bitcoins made is planned to be sliced down in half until 2140 when creation should go to zero. The 21 million limit on the quantity of tokens is expected to make shortage, so as to help valuing of those tokens in standard monetary standards. **Brian P. Hanley**[9] said that even though bitcoin was made with built in shortage, each bitcoin in presence is itself recently created cash. Which he noted as an irony of Bitcoin while bitcoin advocates criticize the capacity of governments to produce cash, bitcoin is a completely made money, which defenders plan to an incentive in fiat monetary forms so as to benefit.

In this paper the authors provide a first deliberate record of chances and restrictions of anti-money laundering (AML) in Bitcoin, a decentralized cryptographic cash multiplying on the Internet. In a progression of investigations, **Malte et al[**10] conducted reverse engineering techniques to comprehend the method of operation and attempt to follow anonymous transactions back to their test accounts. Because of limited number of tests, their outcomes are of exploratory nature, need further substantiation with proof from quantitative estimation examines. Their outcomes likely exaggerate the degree of anonymity gave by the analyzed administrations. This view is upheld by the general warning that clients should completely believe the anonymizing administrations in regards to the privacy (in a perfect world, quick cancellation) of information yield relations and the eagerness to restore the briefly endowed qualities.

# CHAPTER 3: METHODOLOGY

This chapter gives an overview of the different parts of the work chronologically. It mainly discusses the theories, techniques, and step by step workflow of the work.

## CHAPTER 3.1: WORKFLOW

The main difference of Bitcoin from traditional currencies lies in the fact that no one controls Bitcoin as it is decentralized. It allows Bitcoin to be an independent peer-to-peer money system that can function regardless of anyone's wishes. It relies on the combined computing power of the network participants, each of which is equal among themselves — nobody is more or less important than the others. Additionally, it helps bring down the cost of using the system by ideally eliminating fees and transaction times, both of which banks need to stay in business.

No one can have an influence over your money and transactions you send or receive. In contrast, fiat currencies rely on centralized entities like central banks, commercial banks, governments, payment processors like VISA or MasterCard, and other intermediaries. Any of those organizations have an authority to decide whether to approve your transaction, whether you can send money to certain people or organizations, or if the money you're using is legal or not. These processes also include in-depth surveillance and data-sharing on everything you do with your money. Other significant difference is that unlike fiat, Bitcoin is not sovereign. There is nothing backing Bitcoin, which means its value is not attached to any political or economic situation, and it can exist independently outside of the traditional system.

From a well renowned source, it has been seen that bitcoin is having significant price gain than previous year and it is estimated that it is more than 50% between January and February, 2020. Between April and July 2019, bitcoin grows up from $4025 to $13910 and then it gradually decreased until December. [11] Another significant event is coming this year which is halving, where there is a hype that the bitcoin production is about to become half within a few months. For that, the reward money for the bitcoin miners will be reduced to 6.25 BTC, which is currently 12.5 BTC. Previously it was seen that after halving event that occurs every four years, price of bitcoin has risen. So, according to crypto analysts and experts this year Bitcoin’s price will be more sustainable than the last year. [12]

Last but not least, Bitcoin introduces a new dimension of programmability. It means that in the future, Bitcoin transactions can be attached to smart contracts or other programs that execute only after certain conditions are met. Such a feature would allow building additional solutions on top of bitcoin, such as reputation management systems, insurance contracts, or similar. Such contracts would not require any third-party intervention to execute. Essentially, it introduces a new dimension to the concept of traditional cash.

## CHAPTER 3.2: CALCULATION & 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.

### *How much electricity does it take to mine one Bitcoin?*

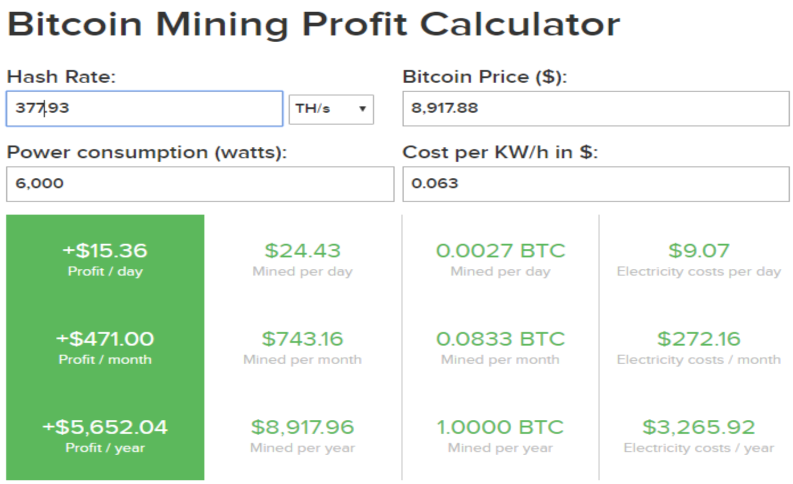
If we run an ASIC (Bitmain Antminer S17) 24/7 for a year it will produce about 0.2646 BTC, at a cost of about 12960 KWh (1500Watt = 1.5 KWh) power in a year. Depending on power prices it will cost anywhere from $816.48 ($0.063 per watt) to mine 0.2646 BTC.

### *How much can you mine Bitcoin in a day?*

There are 144 blocks per day are mined on average, and there are 12.5 bitcoins per block. So everyday about $144 * 12.5 = 1800\text{BTC}$ being mined.

***How much does it cost to mine 1 Bitcoin?***

The cost of mining a bitcoin is subjectable if we use hash rate of 377.93 TH/s which is about 4 ASIC (Bitmain Antminer S17) chip it will cost us about $3265.92 to mine 1 BTC [Electric price is taken as Bangladesh electric price charge which is $0.063 per watt].



Bitcoin Mining Profit Calculator

Hash Rate: 377.93 TH/s

Bitcoin Price ($): 8,917.88

Power consumption (watts): 6,000

Cost per KW/h in $: 0.063

| | | | |
|---|---|---|---|
| +$15.36<br>Profit / day | $24.43<br>Mined per day | 0.0027 BTC<br>Mined per day | $9.07<br>Electricity costs per day |
| +$471.00<br>Profit / month | $743.16<br>Mined per month | 0.0833 BTC<br>Mined per month | $272.16<br>Electricity costs / month |
| +$5,652.04<br>Profit / year | $8,917.96<br>Mined per year | 1.0000 BTC<br>Mined per year | $3,265.92<br>Electricity costs / year |

Fig1: Cost Calculation of ASIC (Bitmain Antminer S17) chip to mine 1 BTC.

***What is the Fastest Bitcoin miner?***

ASIC (Bitmain Antminer S17+ 100TH/s @ 1500W + PSU by PROMINER) has the highest hash rate of 100TH per second with the energy consumption of 1500w.

***How much Bitcoin are left to mine?***

From today’s point of view are 2,741,388 bitcoins left to be mined.

***How Many Bitcoins Are There Now in Circulation?***

There are currently 18,258,613 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 18,258,613 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.

## CHAPTER 3.3: POWER CONSUMPTION & PROFIT CALCULATION

Let’s see how much power it takes to merge 1000 computers to mine a bitcoin.

Let’s assume each has PC has core i7 3.40 GHz clock speed, 500Watt power supply and cost of electricity 0.063$(in BD).

### *Clock Speed Calculation*

1 PC of Core i7 Processor has 3.40 GHz Clock Speed

1000 PC of Core i7 Processor has = $3.40\ \mathrm{GHz} * 1000\ (\mathrm{PC})$

= $3400\ \mathrm{GHz}$

= 3.4 THz [1000 GHz = 1 THz]

So, we can see 3.4 THz Clock Speed needed for 1000 PC

### *Power Consumption Calculation*

1 PC of Core i7 3.40 GHz Processor Consumed 500 Watt Power

1000 PC of Core i7 3.40 GHz Processor Consumed = $500\ \mathrm{Watt} * 1000(\mathrm{PC})$

$= 500000\ \mathrm{Watt}$

$= 0.5\ \mathrm{MWh}$

$= 500\mathrm{KWh}$ [1000 KWh = 1 MWh]

***Hash rate Calculation***

1 PC of Core i7 3.40 GHz Processor  has Hash Rate 291 h/s

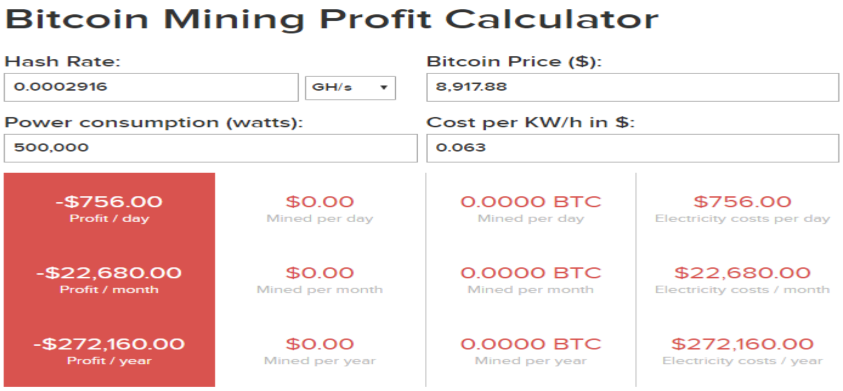
1000 PC of Core i7 3.40 GHz Processor has Hash Rate $= \ 291\ h/s\ *\ 1000(PC)$

$$= 291000\ h/s$$

$$= 0.0002916\ GH/s[1\ GHz = 10\text{\^{}}9\ hs]$$

***Profit Calculation***

So, we can see that if 1000 core i7 3.4GHz PC used, it will needed 5,00000 Watt or 500 KWh or 0.5 MWh power with the price of $0.063 per watt ,which will produce -$756.00 in a day which is a negative rate that means it will not give us profit but it will make us lose our money.



Bitcoin Mining Profit Calculator

Hash Rate: 0.0002916 GH/s

Bitcoin Price ($): 8,917.88

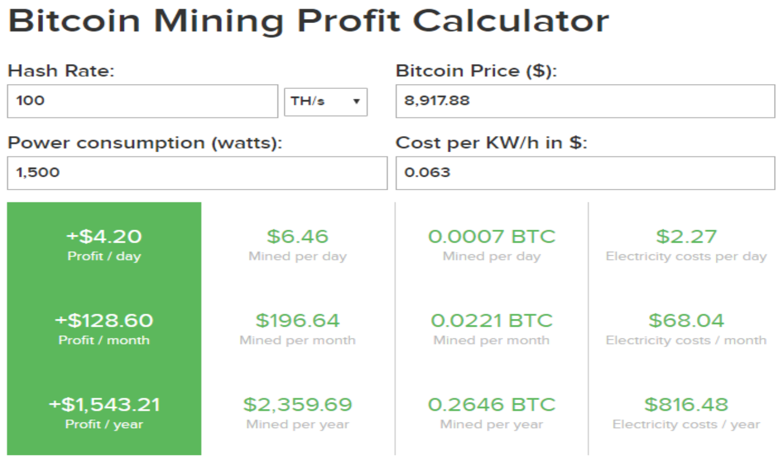
Power consumption (watts): 500,000

Cost per KW/h in $: 0.063

| | | | |
|---|---|---|---|
| -$756.00<br>Profit / day | $0.00<br>Mined per day | 0.0000 BTC<br>Mined per day | $756.00<br>Electricity costs per day |
| -$22,680.00<br>Profit / month | $0.00<br>Mined per month | 0.0000 BTC<br>Mined per month | $22,680.00<br>Electricity costs / month |
| -$272,160.00<br>Profit / year | $0.00<br>Mined per year | 0.0000 BTC<br>Mined per year | $272,160.00<br>Electricity costs / year |

Fig 2: Profit Calculation of 1000 Core i7 2.4 GHz PC

Now see, if we use an ASIC (Bitmain Antminer S17) chip it has $100^{TH}$/s or 100000 GH/s and it consumes only 1500 Watt power with the price of $0.063 per watt, which will produce $4.20 profit per day and $128.60 profit per month. Which is profitable



Bitcoin Mining Profit Calculator

Hash Rate: 100 TH/s

Bitcoin Price ($): 8,917.88

Power consumption (watts): 1,500

Cost per KW/h in $: 0.063

| | | | |
|---|---|---|---|
| +$4.20<br>Profit / day | $6.46<br>Mined per day | 0.0007 BTC<br>Mined per day | $2.27<br>Electricity costs per day |
| +$128.60<br>Profit / month | $196.64<br>Mined per month | 0.0221 BTC<br>Mined per month | $68.04<br>Electricity costs / month |
| +$1,543.21<br>Profit / year | $2,359.69<br>Mined per year | 0.2646 BTC<br>Mined per year | $816.48<br>Electricity costs / year |

Fig 3: Profit Calculation of ASIC (Bitmain Antminer S17) chip.

| **Criteria** | **1000 PC of Core i7 3.4 GHz** | **ASIC(Bitmain Antminer S17) chip** |
|---|---|---|
| Hash Rate(GH/s) | 0.0002916 GH/s | 100 TH/s |
| Power Consumption | 500000 Watt | 1500 Watt |
| Heat generated | Very High | Comparatively low |
| Profit/Loss (Per day) | -$756.00 (Loss) | +$4.20 (Profit) |

Table 1: Difference between 1000 PC of Core i7 3.4 GHz and An ASIC (Bitmain Antminer S17) chip.

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.

## CHAPTER 4: CONCLUSION

Bitcoin is the popular cryptocurrency with a big user base and podded network, all hinging on incentives in place to retain the important bitcoin block chain. Bitcoin is a latest cryptocurrency that anybody try to pulling out. There are number of reason people try to mining the currency. Bitcoin mining is the most difficult and long process where people can attach a block of transaction to the bitcoin block chain without needing consent form any authority and gate rewarded in bitcoin for it. The many complexity increases with the network hashing power so normal pc does not handle it. It is possible to mine bitcoin merging many normal pc but it is very costly.

## CHAPTER 4.1: SUMMARY

Nowadays cryptocurrencies are getting popular day by day. Finding its actual source of resource and how it works might help all people who are getting used to money transaction via online. And it will help people to maintain precaution when they need to transfer any big amount transactions.

## CHAPTER 4.2: FUTURE WORK

In future we want to implement this project in real-world. We would like to collaborate our work with machine learning technology to see if we can make a prediction actually when will be the end of the bitcoin and how much 1btc would cost in future in terms of dollar and what type of GPU would be good to mining. And we also would like to work on other cryptocurrencies like ETH and LTC.

## APPENDIX

There are total eight type of cryptocurrencies till now.

BTC = “Bitcoin”

*One of the most commonly known currencies, Bitcoin is considered an original cryptocurrency.*

LTC= “Litecoin”

*Litecoin was launched in 2011 as an alternative to Bitcoin.*

ETH=”Ethereum”

*Created in 2015, Ethereum is a type of cryptocurrency that is an open source platform based on blockchain technology.*

XRP=”Ripple”

*Ripple was released in 2012 that acts as both a cryptocurrency and a digital payment network for financial transactions.*

Bitcoin Cash

*Bitcoin Cash is a type of digital currency that was created to improve certain features of Bitcoin. Bitcoin Cash increased the size of blocks, allowing more transactions to be processed faster.*

Ethereum Classic

*Ethereum Classic is a version of the Ethereum blockchain. It runs smart contracts on a similar decentralized platform. Smart contracts are applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interface.*

*ZEC= “Zcash”*

*Zcash is a digital currency that was built on the original Bitcoin code base. Conceived by scientists at MIT, Johns Hopkins and other respected academic and scientific institutions, it was built on a decentralized blockchain. A core feature and differentiation of Zcash is an emphasis on privacy. While not a function available to investors on Equity Trust’s platform, users can send and receive Zcash without disclosing the sender, receiver or the amount transacted.*

XLM=”Stellar Lumen”

*Stellar lumen is an intermediary currency that facilitates currency exchange. Stellar allows a user to send any currency they own to someone else in a different currency. Jed McCaleb founded the open-source network Stellar and created the network's native currency in 2014.*

Best Software to mine Bitcoin

- *BTCMiner is an open Source Bitcoin 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.*

## REFFERENCES

[1] ‘Types’. [Online]. Available at: https://www.trustetc.com/blog/cryptocurrency-types/

[Accessed 21- Sep- 2018].

[2] Christian Decker & Roger Wattenhofer, “Information Propagation in the Bitcoin Network”, 2013, 13-th IEEE International Conference on Peer-to-Peer Computing.

[3] Andrew Miller, et al, “Permacoin: Repurposing Bitcoin Work for Data Preservation”, 2014, IEEE Symposium on Security and Privacy, Doi: 10.1109/SP.2014.37

[4] Dorit Ron and Adi Shamir, “Quantitative Analysis of the Full Bitcoin

Transaction Graph”, 2013, 17th International Conference on Financial Cryptography and Data Security.

[5] Andrew Miller, et al, “Nonoutsourceable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions”, October 2015, the 22nd ACM SIGSAC Conference, DOI: 10.1145/2810103.2813621

[6] Jae Kwon, “Tendermint: Consensus without Mining”, 2014, Computer Science, https://pdfs.semanticscholar.org/df62/a45f50aac8890453b6991ea115e996c1646e.pdf

[7] Ian Miers, et al, “Zerocoin: Anonymous Distributed E-Cash from Bitcoin”, 2013, IEEE Symposium on Security and Privacy, https://doi.org/10.1109/SP.2013.34.

[8] Malte M¨oser, et al, “Towards Risk Scoring of Bitcoin Transactions”, March 2014, International Conference on Financial Cryptography and Data Security, DOI: 10.1007/978-3-662-44774-1_2.

[9] Brian P. Hanley, “The False Premises and Promises of Bitcoin”, December 2013, New banking and novel currency, https://arxiv.org/ftp/arxiv/papers/1312/1312.2048.pdf.

[10] Malte Möser, “An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem”, September 2013, APWG eCrime Researchers Summit, https://doi.org/10.1109/eCRS.2013.6805780

[11]https://www.tradingview.com/chart/?symbol=COINBASE%3ABTCUSD

[12]https://www.forbes.com/sites/benjaminpirus/2020/02/20/bitcoins-2020-rally-more-sustainable-than-2019-surge/#22bd69b633a6