TITLE

“DISSERTATION ON CRYPTOCURRENCY MINING SYSTEM”

SUBBMITED BY

1) HARSHIL MANDALI A28
2) PRIT SHAH A58
3) SAGAR SUTHAR B58

GLS UNIVERSITY

Faculty of Computer Applications & Information Technology

***i*MSc(IT) Programme**

Ahmedabad

CERTIFICATE

This is to certify that

1) MANDALI HARSHIL A 28
2) PRIT SHAH A58
3) SAGAR SUTHAR B58

Student/s of Semester- VI Integrated Msc(IT) [TY iMSc(IT)], FCAIT, GLS University has/have successfully completed the

Dissertation

on

"**Cryptocurrency Mining System**"

as a partial fulfilment of the study of Third year Semester-VI, **Integrated Master of Science (Information Technology) [*i*MSc(IT)]**

Date of Submission: 14-03-2022

Prof. Neha Vaswani	Prof. Tripti Dodiya
(Project Guide)	(Project Co – Ordinator)

Acknowledgement

I would like to express my special thanks of gratitude to Our project Guide Prof. Neha Vaswani For Guiding us throughout the course of the project Also, we would like to thank Prof. Tripti Dodiya for providing our group this opportunity for completing this project.

Index

INTRODUCTION

A cryptocurrency is a digital currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it.

Individual coin ownership records are stored in a digital ledger, which is a computerized database using strong cryptography to secure transaction records, to control the creation of additional coins, and to verify the transfer of coin ownership

Some crypto schemes use validators to maintain the cryptocurrency. In a proof-of-stake model, owners put up their tokens as collateral. In return, they get authority over the token in proportion to the amount they stake. Generally, these token stakers get additional ownership in the token over time via network fees, newly minted tokens or other such reward mechanisms.

Cryptocurrency Mining

Bitcoin network is secured by individuals called miners.

Any machine in the Bitcoin network can act as a miner. Users have used several types of hardware over time to mine blocks of Bitcoin.

CPU mining, GPU mining, FPGA mining and ASIC mining are popularly used hardware for Bitcoin mining. All the hardware mining has to deal with low profit, excess heat and high electricity cost.

Cloud mining is another solution to these problems since it does not have to deal with excess heat or high electricity cost.

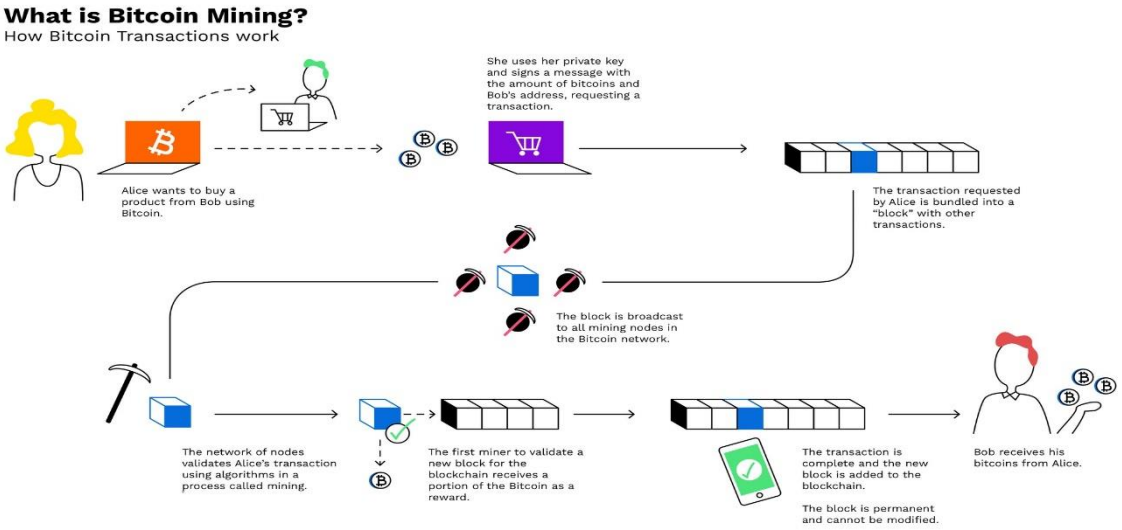
But it has few other limitations. The miner uses its processing power to solve the puzzle and broadcast on the network. Bitcoin mining is the process of adding transaction records to Bitcoin's public ledger of past transactions or blockchain. A transaction is only considered to be valid when it is signed by the sender.

Mining is done by the miners who are watching Bitcoin transaction continuously and trying to verify it.

As there are more miners added to the network, the challenge gets actually harder and harder, in such a way that in the average of 10 minutes, a new block of a transaction is added to the blockchain in the network. A block is only considered valid when it has proof of work. The miner who mines the block gets a reward.

The new Bitcoins are obtained by miners as a reward and also the transaction fee obtained from all the transactions included in the block.

This motivates the miners to continuously compete in the race for finding a valid block.



Hardware for Bitcoin Mining

Bitcoin miners utilize their assets (equipment and power) to approve an exchange, and new Bitcoin are produced in the organization each time a block is mined. Following are the manners in which that portray utilization of various strategies for mining cryptographic money

CPU Mining

Everything you need to use the CPU method to be able to mine is just a CPU and a couple of programs. Miners used standard processors to overcome the mathematical problems in the early days of Bitcoin, managing processor units (CPUs). It used to require some investment for mining Bitcoin and other cryptographic forms of money, despite the fact that the difficulty levels were less difficult than today. The degree of difficulty proceeds to change and grow, so the excavators have needed to build their preparing power too.

Cloud Mining

Cloud mining is likely the most famous route to mine digital currencies. Cloud mining has become so mainstream to a great extent since it gives individuals who might not have sufficient cash to purchase their hardware or who may essentially not be keen on claiming an equipment's the capacity to take an interest in the realm of digital currencies.

A few hosts give you the choice to assemble and design your cloud mining plan. At that point look at the plans that the host gives and go through with the exchange (which T. Pawar et al. / A Survey on Mining Cryptocurrencies 333 means you pay the host), register digital currency wallet code and that is initial steps to mine

GPU Mining

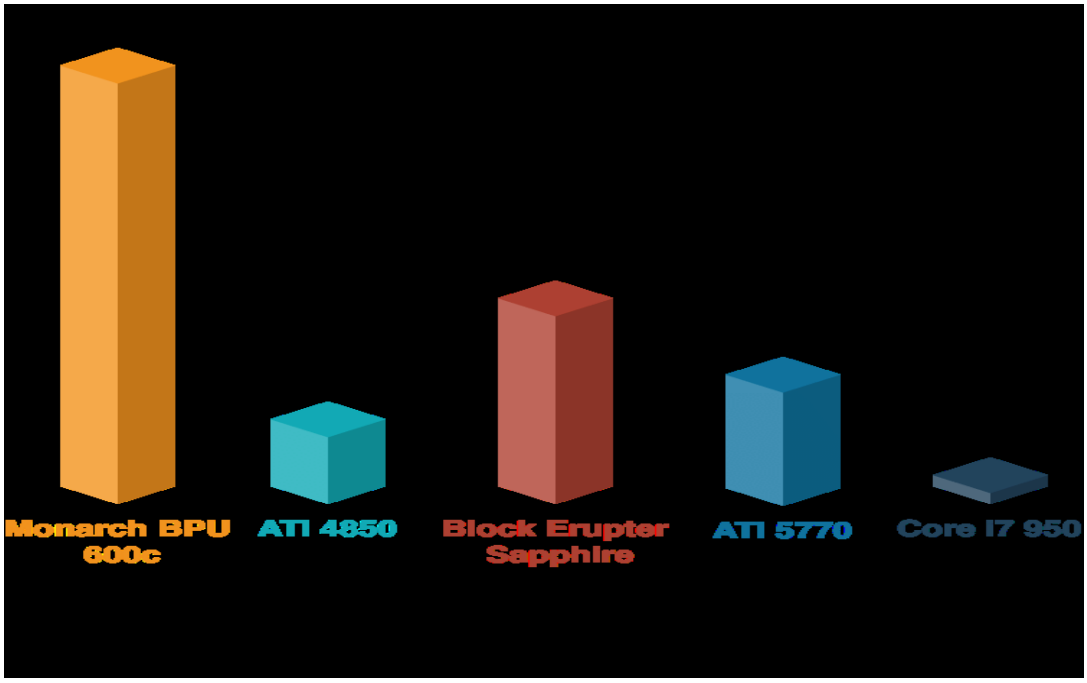
The most mainstream and notable strategy for mining cryptographic forms of money is presumably GPU mining. GPU mining is likely the most widely recognized and notable interaction for mining digital forms of money. Designs cards are utilized by GPU apparatuses to mine cryptographic forms of money.

A processor, a motherboard, cooling, rig outline and - obviously - a couple (2 - 8) illustrations cards are made of one single apparatus. A normal cost for a well-performing and pleasantly planned GPU mining rig will in general be around the $3000 value range.

ASIC Mining

Miners use ASIC (application-explicit incorporated circuit) innovation, which was presented explicitly for mining Bitcoin and other digital forms of money. ASICs are very notable and regarded in light of the fact that they make insane amounts of cryptographic money contrasted with the GPU and CPU of their rivals. They burglarize different diggers who use GPU or CPU apparatuses of the capacity to stay aware of both hash paces and income.

ASICs have additionally turned some remarkable cryptographic forms of money's economy - imagine if the bulk of profit will go to one miner with an ASIC ranch



Latest and Popular types of Minable Cryptocurrency

Bitcoin - bitcoin miners use powerful computers to verify blocks of transactions and generate more bitcoins — a complex, time-consuming process called proof-of-work (PoW).

Minable With CPU GPU

ECOS - The company provides both options – ASIC mining and cloud mining.

Vertcoin - VerthashMine software is to be used to mine the crypto. It is not mineable with ASICs or CPU cards

Grin - Can be mined with Gminer, Grin Goldminer, Cudo Miner, and lolMiner GPU mining software. These are downloadable for free

Can be mined through solo mining with ASICs.

Monero - Does not use too much power when mining with CPUs.1 Monero is mined every 24 seconds. The reward for miners is around 4.99 XMR

ZCash - ASIC resistance. Can be mined best by GPUs using EWBF ZCash Miner Windows miner. Mineable with CPUs making it very cost-effective for beginners.

Raven coin - Cannot be mined with ASICs, hence allowing people to mine at low initial costs.

Haven Protocol - It inherits Monero's privacy features such as RingCT and stealth addresses. Hence, it can be used for private sending and receiving.

Ethereum Classic - Mainly mined with Ethminer, Claymore Miner, FinMiner, GMiner, and NBMiner GPU miners. Cruxminer, GMiner, lolMiner, Nanominer, NBMiner, and OpenETC Pool, are also some of the software you can use to mine ETC

Litecoin - For ASIC miners, the software will most likely be pre-installed in the hardware. Otherwise, you can use the free ASIC/FPGA miner or other software.

Litecoin mining pools include Litecoinpool, MinerGate, LTC.top, Antpool. F2pool, and ViaBTC

Ethereum - Can be mined with ETHminer, CGMiner, WinEth, BFGMiner, Geth, EasyMiner, T-Rex, and Lolminer. It is not profitable to mine with a CPU

Monacoin - Not able to be mined with ASICs.

Software used to mine this cryptocurrency includes Lyra2REv2 miner, XMR Stak, CGminer, CCMiner, and Suprnova.

Bitcoin Gold - Software used to mine this cryptocurrency includes Lyra2REv2 miner, XMR Stak, CGminer, CCMiner, and Suprnova.

Minable with GPU

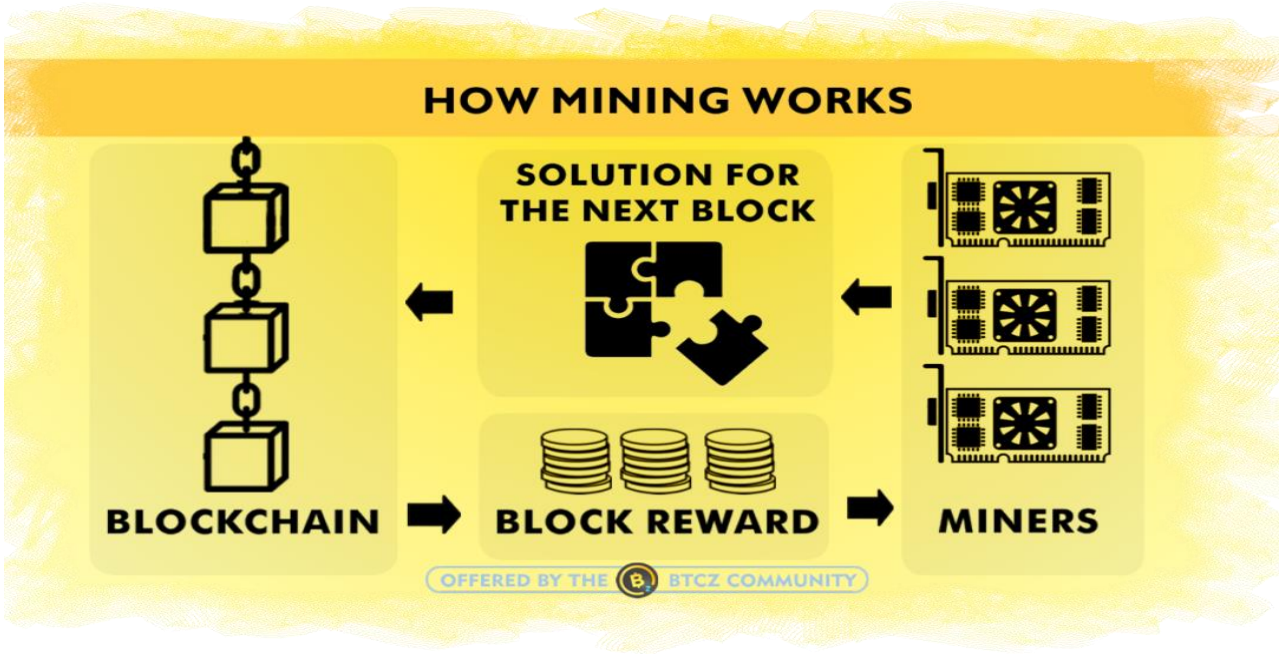
Aeternity - Options to mine with GPUs, CPUs, ASICs

It takes about 3 minutes to confirm a block on the Aeternity blockchain. The reward per block mined is 124 AE.

Types of mining technique

1. **Proof of Work (Pow)**
2. **Proof of Stake (PoS)**

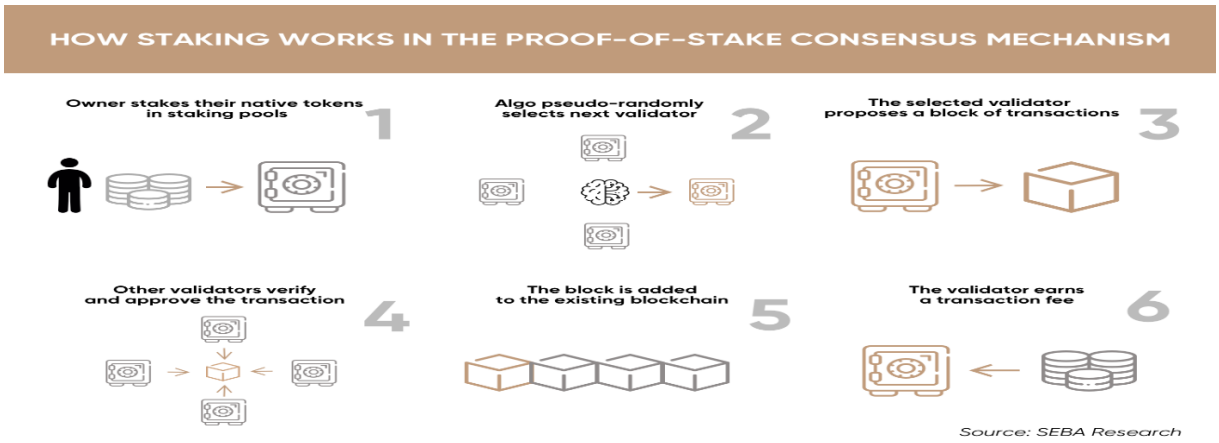
1. **What is Proof of Work (Pow) -** Proof of Work (Pow) may be a protocol designed to form digital transactions secure without having to believe a 3rd party.
2. This work builds on previous puzzle solutions. Pow may be a way of verifying current and past transactions. The work that goes into solving puzzle generates rewards for whoever solves it called it as mining.
3. In other words, this is often an algorithm that's designed to verify transactions and obtain new blocks added to blockchain.
4. With Proof of Work, miners are competing to be primary to finish a complex mathematical puzzle which will generate this new block, meaning that they'll be ready to collect some new Bitcoins as a rewards.



Features

- PoW reduces risk of a 51% attack because it’s very hard to do work.
- No miner will be able to control bitcoin network single handedly Based on Hashcash PoW system.
- The miners need to give a proof that they have done some work, before proposing a new block.
- At the same time, each solution is easy for community to verify. This makes it easy to check all transactions for trustworthiness.
- PoW also sets a limit on how many new blocks of data can be generated. For example, miners can only create a Bitcoin (BTC) block every 10 minutes.
- It doesn’t rely on a single third-party transactor. This builds a “trustless” and transparent network.
- Monopoly can increase over time.

2. What is Proof of Stake (PoS)? – Proof-of-stake is a consensus algorithm that decides on who validate next block, according to how many coins you hold, instead of miners cracking cryptographic puzzles using computing power to verify transactions like they do with traditional Proof-of-Work.



Features

- The probability of validating a new block is determined by how large a stake of a person.
- The validator does not receive a block reward, instead they collect network fees as their reward.
- Peercoin was first cryptocurrency to implement a full-scale PoS consensus model.
- Handling Monopoly and Power Consumption.

Difference between Proof of Work (PoW) and Proof of Stake (PoS) in blockchain:

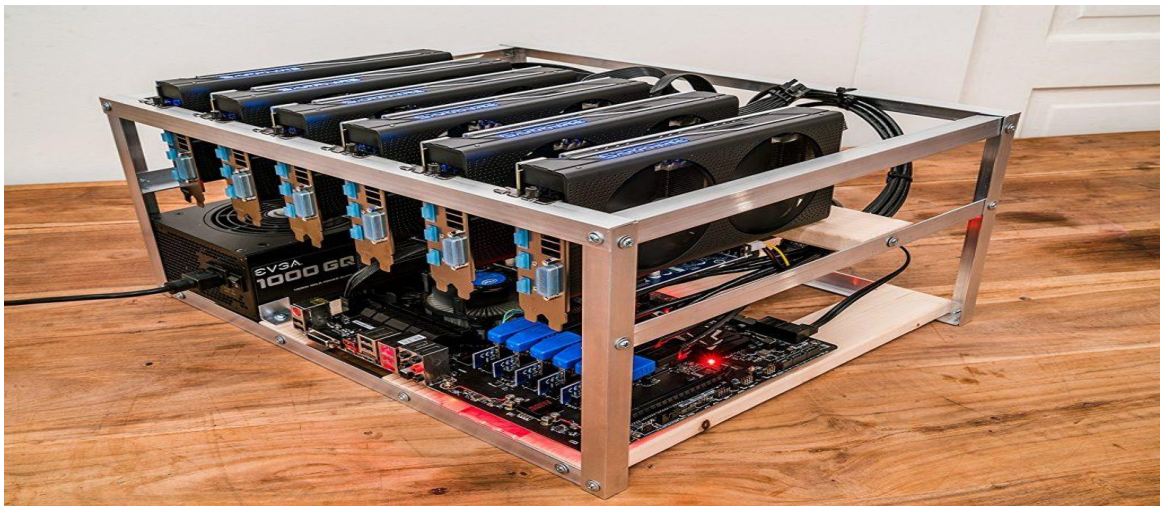
	Proof of Work (PoW)	Proof of Stake (PoS)
1.	The probability of mining a block is determined by how much computational work is done by miner.	The probability of validating a new block is determined by how large of a stake a person holds (how many coins they possess).
2.	A reward is given to first miner to solve cryptographic puzzle of each block.	The validator does not receive a block reward instead they collect network fee as their reward.
3.	To add each block to chain, miners must compete to solve difficult puzzles using	There is no competition as block creator is. chosen by an

	their computer process power	algorithm based on user stake.
4.	Hackers would need to have 51% of computation power to add malicious block.	Hackers would need to own 51% of all currency on network, which is practically impossible.
5.	Proof of work systems are less energy efficient and are less costly but more proven.	Proof of Stake systems are much more cost and energy efficient than POW systems but less proven.
6.	Specialized equipment to optimize processing power.	Standard server grade unit is more than enough.
7.	Initial investment to buy hardware.	Initial investment to buy stake and build reputation.
8.	Bitcoin is most well-known crypto with a Proof-of-Work consensus building algorithm which uses most well-known proof-of-work function is called SHA256.	Some of cryptocurrencies that use different variants of proof-of-stake consensus are: EOS (EOS), Tezos (XTZ), Cardano (ADA), Cosmos (ATOM).

Cryptocurrency Mining-rig

A mining rig is a computer system used for mining bitcoins. The rig might be a dedicated miner where it was procured, built and operated specifically for mining or it could otherwise be a computer that fills other needs, such as performing as a gaming system, and is used to mine only on a part-time basis.

In simple words mining rig is many graphics cards are attached in one rig to produce more Hash rate, compare to single graphics card to make mining more profitable, Also easy to carry from one place to other, And avoiding mess in wires.



Advantages of Mining a Cryptocurrency

Bitcoin mining and other cryptocurrencies have several advantages. Unlike traditional banks that can freeze your assets, you have full control over your Bitcoins at all times. This can be lost if you misplace your private key. Other highlights of cryptocurrency include:

- Inability to counterfeit
- Lower fees
- Access by everyone
- Immediate settlement (third parties are eliminated when closing on a new home)
- End to identity theft (credit uses a pull method to access funds while cryptocurrency pushes it through)

With the use of cryptocurrency, you'll never have to worry about someone stealing the RFID information in your credit or debit card at the checkout! It will also completely put an end to identity theft. Bitcoin can't be counterfeited, because it's digital currency. This will ultimately lower the cost of goods and services globally as more and more people use it.

- In Cryptocurrency mining, its main advantage is once miner setup its Mining hardware's and software after that there is no maintenance or time consuming. Just they have to clean graphic cards once a week

- It is one time Investment, after purchasing mining rig or graphics cards for crypto mining they are very durable and have long lasting life.
- Fast return of investment, Amount of money miner invested for buying mining rig, that returns back in only 1 or 2 Months.
- One-time setup, it can be difficult to setup for first time but after that it work on its own.
- It generates employment, Number of people started mining farm and also made it business
- Now mining is a type of business-like people who have knowledge about mining graphics cards, how to start mining, they make mining rig and according to customer budget they sell them, After they help customer or charge from customer to getting setup mining farm.
- Company or Individual who sell mining rigs help customer to combine all mining rigs and graphic cards, and pc contain ram rom, CPU, monitor in that way they can easily mine crypto without any problem.
- And its main advantage is once they setup all things no need to see regularly it. Customer only need to clean setup once a week because if dust will be jammed in fan it can cause problem of heating and low performance.

Disadvantages of Mining a Cryptocurrency

- you need to learn when you start your journey as a miner. Because “all that shines is not perhaps glitters”.
- The blockchain technology that which is responsible for all the behind-the-scenes work is also not easy and needs proper handling because the process is going to take a lot of learning to get your hands on it.
- The lot most spoken demerit is the energy consumption that it uses for mining cryptocurrency along with hardware expenses.
- Lastly, we have seen that the crypto industry is Although the money that a person incurs from mining and the security that it provides has always been ranted about there is a sometimes flooded with scams and frauds which in future can create upheaval. Also, there are fair chances of you losing your money due to the volatility and constant fluctuation of the cryptocurrency market bringing bad luck to you in the crypto investments.
- High investment cost- Components like graphics card and mining rig are most expensive in mining, Normal people or individual cannot afford them
- It is non profitable for small scale or individual to mine crypto, because using 1 or 2 graphics card it consumes more electricity and produce less hash rate so profit become very less and investment value will return in very long time High knowledge is required, because not

anyone can buy mining equipment and start mining, they should have knowledge of mining software's and how to start mining, that is very difficult to setup at first.

- Electricity consumption, In mining process consume high amount of energy or electricity so miners need to have proper and stable electricity and in high amount to mine crypto. Heating problem, Miners have to take care of temperature while in mining process, Because mining equipment heat so much, so they have to control room temperature during mining
- Cleaning graphics cards and mining rigs, Miners have to make sure to clean their rooms or mining farms and protect rigs and cards from unwanted dust and mud, and have to clean them time to time if not done so it can create problem in mining.
- Mining BAN problem, Because of high electricity consumption countries are banning crypto mining, Countries are facing electricity shortage, So if miners country ban crypto mining they have to migrate to another country, And start again whole setup of mining.
- Electricity cost of country, Crypto miners have to check in which country there is cheap electricity, so In low electricity cost they can mine and make profits, and if they mine in high electricity chargeable country their whole profit money will go in paying electricity charge.
- Mining rewards, Year by year mining rewards get less or gets half than before so profits are getting lower and lower

How to overcome Disadvantages

- High-cost equipment – mining equipment are very costly so beginner person can start mining with small scale and with partner so cost will be divided and from mining profit they can buy more rigs and graphics cards.
- High knowledge is required as miner- After purchasing mining setup how to run is important so for that high knowledge is required, So Miner who purchased equipment from company they provide person to help the setting up everything will it work fluent and properly and its only one-time setup.
- High Electricity consumption – In crypto mining it is most important problem miners face high electricity consumption = high electricity bill = less profit, Miners have to take care of electricity charges, So this problem can be solved using “Solar panels” by using solar panels natural source of energy electricity problem can be solved
- Heating problem – It is second major problem in mining graphics cards become hot while mining process so miners have to keep setup at cooler place, and by putting multiple fans during summer

and cut off AC can solve this problem so room temperature can be maintained

- ❖Cleaning problem – miners have to take care of mud and dust coming from outside windows, But it is less time-consuming process they have to clean it once a week by help of Blower.
- ❖Mining Ban problem- Miners have to migrate from one country to another if a country bans mining, That's only solution of it. And they should pick that country that supports mining like Russia
- ❖Mining Rewards or Block Reward Halving – As mining reward is getting less year-by-year miners should be shifting to other crypto minable coins. Eg
- ❖The block reward of bitcoin mining at the foremost events of the invention was 50, later the foremost block reward halving took place in 2012, and the block reward was condensed by 25 bitcoin units, and the progression continued for every four years, the current block reward of bitcoin mining is 6.25. Despite these facts, bitcoin miners generated a revenue of 60 million per day in the month of April, the second strongest month in terms of bitcoin mining.

Conclusion

Cryptographic forms of money are decentralized and run on the guideline of blockchain.

Every one of the exchanges is reasonable and straightforward.

The pace of trouble and the opposition between the excavators with the best accessible equipment makes mining more complicated. Digital currency mining needs a great deal of

Figurering and great equipment that can give a great hash rate with low energy.

Miners should be cautious about picking equipment prior to beginning to mine digital

money due to equipment costs. It is exceptionally high and the other extra expense

during mining is the expense of power and fixes.

References

- https://www.researchgate.net/publication/331040157_A_Survey_on_Bitcoin_Cryptocurrency_and_its_Mining
- https://www.researchgate.net/publication/356755723_A_Survey_on_Mining_Cryptocurrencies
- https://www.softwaretestinghelp.com/best-cryptocurrency-to-mine/
- https://www.geeksforgeeks.org/difference-between-proof-of-work-pow-and-proof-of-stake-pos-in-blockchain/
- https://academy.bit2me.com/en/what-is-mining-rig/#:~:text=A%20mining%20rig%20is%20an,arranged%20to%20perform%20cryptocurrency%20mining
- https://moneyminiblog.com/investing/advantages-of-bitcoin-mining/
- https://www.researchgate.net/deref/https%3A%2F%2Fwww.nytimes.com%2Finteractive%2F2021%2F09%2F03%2Fclimate%2Fbitcoin-carbon-footprint-electricity.html