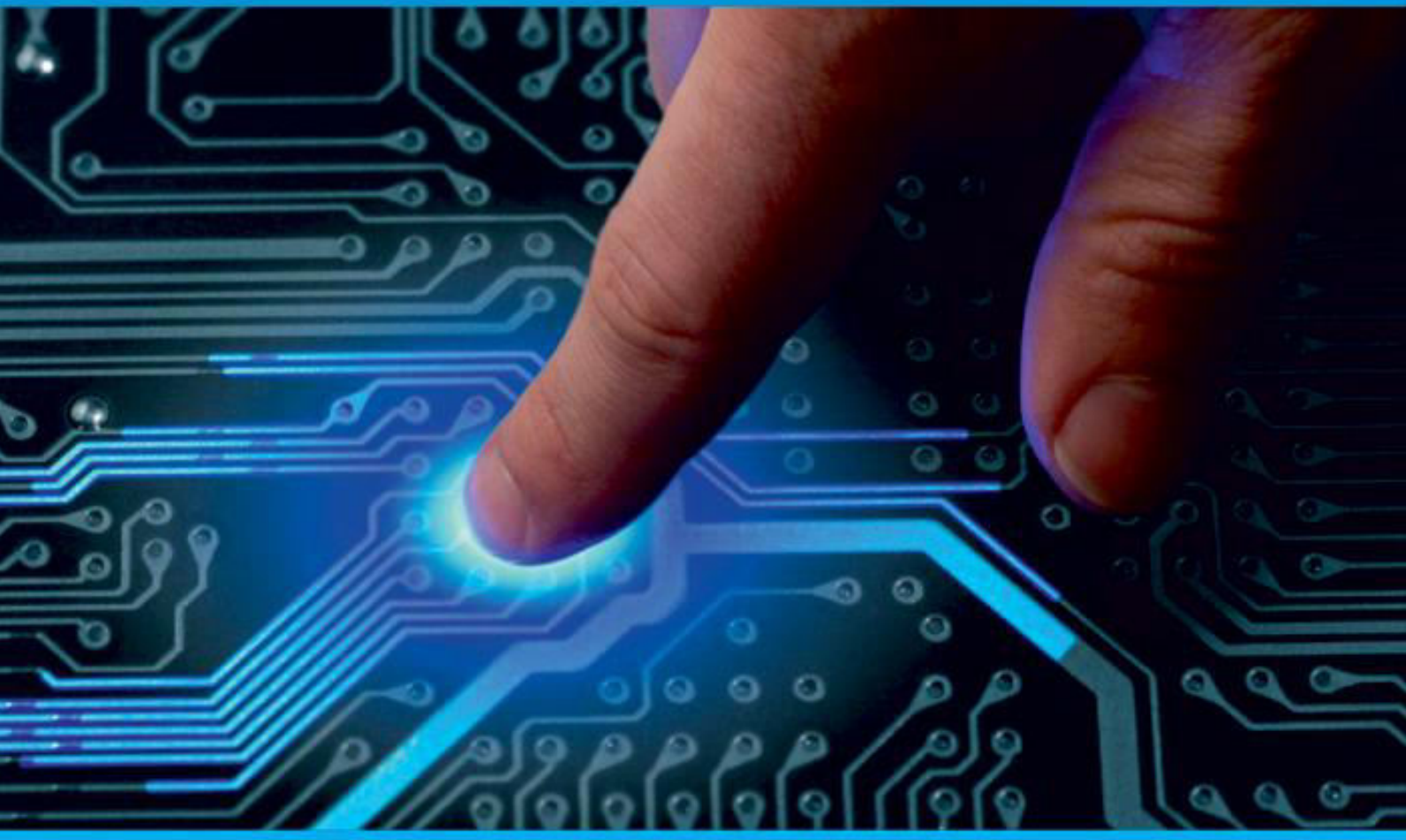
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 9, September 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009028 |

Implementation of Bitcoin System and BTC Mining Operation

Ms. VIDYA S.I [1], Dr. Mohamed Rafi [2]

PG Student, Department of Computer Engineering, UBDTCE, Davanagere, India [1]

Professor, Department of Computer Engineering, UBDTCE, Davanagere, India [2]

ABSTRACT: Bitcoin Mining software's are specialized tools which uses your computing power in order to mine cryptocurrency. In exchange of mining operation, you can receive a monetary reward in the form of digital currency. These applications provide a detailed report based on your earnings. The majority of these software programs are automated and one does not need technical skills to use them. It allows you to manage all your activities remotely. This Bitcoin miner app enables you to check mining status with ease. This application contains charting tools to track trends and price movements.

KEYWORDS: Blockchain, Cryptocurrency, Bitcoin, Bitcoin mining, Transaction.

I. INTRODUCTION

Bitcoin emerged out of the 2008 global economic crisis when big banks were caught misusing borrowers' money, manipulating the system, and charging exorbitant fees. To address such issues, Bitcoin creators wanted to put the owners of bitcoins in-charge of the transactions, eliminate the middleman, cut high interest rates and transaction fees, and make transactions transparent. They created a distributed network system, where people could control their funds in a transparent way.However, there are issues with bitcoins such as hackers breaking into accounts, high volatility of bitcoins, and long transaction delays. Elsewhere, particularly people in third world countries find Bitcoins as a reliable channel for transacting money bypassing pesky intermediaries.

Bitcoin is unlike anything the world has seen before. By providing fast, inexpensive, international money transfer, it has the potential to revolutionize both the modern-day concept of money and commerce. Bitcoin started as a free software project and a paper published by Satoshi Nakamoto in 2009. Nakamoto, who seems to have been created specifically to deliver Bitcoin to this world, designed a system of online value transfer that supports a promising Internet currency.

Bitcoin is made possible by a combination of software and network technologies. A program called the Bitcoin client simultaneously manages and helps you spend bitcoins. This program maintains a long ledger called the blockchain that holds every transaction confirmed by the Bitcoin network.

Figure 1. shows blockchain working process.That first connect using a Bitcoin client, then try to verify those transactions by analyzing blocks of data, or hashes. The transmission of information takes place through a number of nodes, which are merely data blocks. Additionally, a miner must verify the accuracy of his solutions because the data is encoded.A transaction is successful after the nodes are confirmed, and the miner is rewarded with some Bitcoins. Simply put, you are participating in an online conference as a bank clerk with numerous other bank clerks. Whoever authenticates the deal makes money. It takes an average of 10 minutes for the right answer to appear, and miners from all over the world compete to be the first to match their hash with it. The mathematical brainteaser is made to automatically change the level of difficulty.

What is Bitcoin Mining?

Bitcoin mining refers to the process of digitally adding transaction records to the blockchain, which is a publicly distributed ledger holding the history of every bitcoin transaction. Mining is a record-keeping process executed through immense computing power. Each Bitcoin miner around the world contributes to a decentralized peer-to-peer network to ensure the payment network is trustworthy and secure.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009028 |

To securely add to the blockchain ledger, Bitcoin mining computers solve complex mathematical problems. When a solution is found, the latest block of confirmed transactions is added as the next link in the blockchain.

As an incentive to mine and contribute to the network, the miner who solved the problem is rewarded a block of Bitcoin.

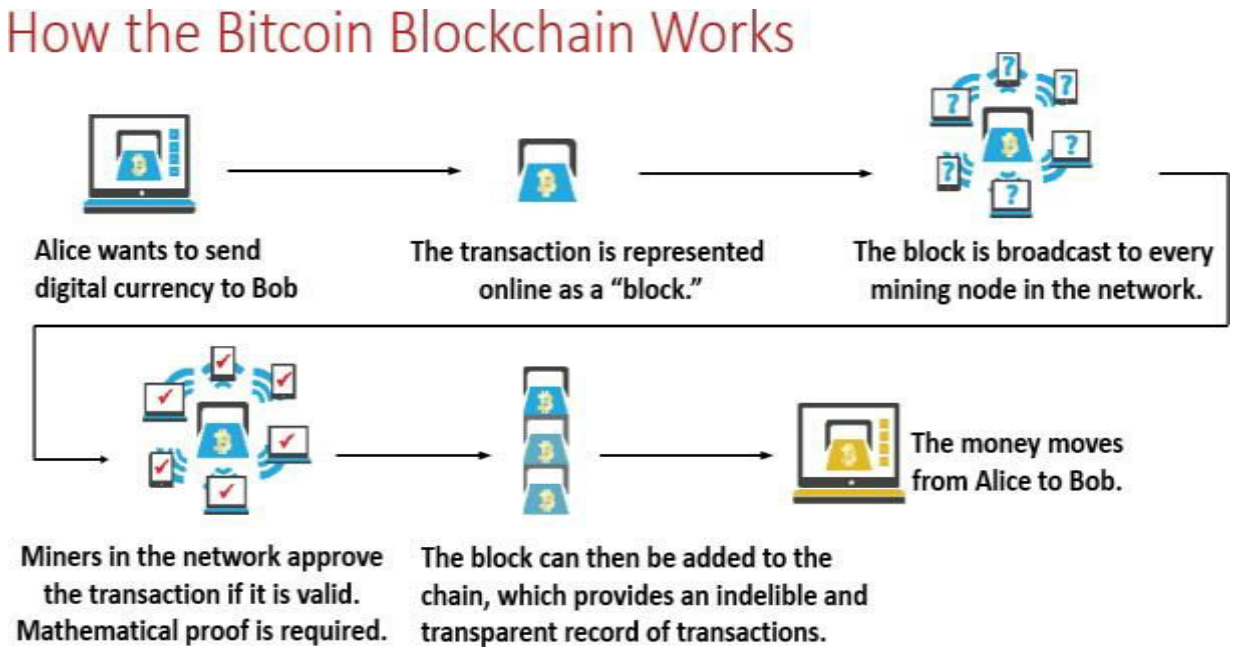


Figure 1. Workflow of Bitcoin blockchain

Why Does Bitcoin Mining Use Energy?

How Is Energy Spent to Mine Bitcoin?

Energy is spent in the form of electricity, which powers the computers of Bitcoin miners. These miners try to add new blocks of transactions to the blockchain, by essentially creating as many tickets to a "lottery" as possible. The winner of this "lottery" is the first one to get the majority of the nodes in the network to verify their block. They are rewarded with newly minted bitcoin and transaction fees to compensate them for their service. Miners then need to use this new block to try to be the first to create the next block in the chain.

A miner must first create a valid block to get a chance at being compensated. By design, creating a block requires energy. When a miner presents a block to the network, they are proving that they put in the work. They can't fake the creation of a valid block, as the nodes in the network would detect it. As a result, none of the network participants have to trust each other, they only need to verify that no rules were broken and all the blocks are valid.

How Does Mining Work?

A miner's block will become a part of the chain whenever a majority of the community of miners agree

(A) The transactions listed by the miner are valid—no signatures from impersonators and no double spending.

(B) The miner correctly guessed a special number, the nonce, that solves a particular math problem. Miners perform this check by looking at the proposed block's particular digital signature.

This signature is a computer generated product of three inputs.

(1) The signature of the predecessor block,

(2) A list of valid transactions since that predecessor

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009028 |

(3) A particular random number, called a nonce.

Signatures operate by using "hash" functions. At their simplest, hash functions are math equations that take any given input and create a seemingly random output that will always correspond to that particular input.

If a hash function is well written, any change to the inputs will drastically change the output string, and different inputs would never output the same string. By that standard, SHA256 is very well written.Below Figure 2. will shows the example of hash function.

"This is a hash!" =
"dcc67309a9c5c4a6d5434de87dbd4162f745f32b2a6aedf89c89d31d863b022b"

"This is a hash?" =
"d43edbde4b15a97e780c1a9e1392b2c4601750fe03db543b3c4c44624d277641"

"This is a hash brown." =
"5692e888b50c526f7eb95342a6fd56760b2ff95a766414562daa4083bab8bcfc"

Figure 2. Hash function examples,change to the inputs will drastically change the output string.

II. LITERATURE REVIEW

1. Bitcoin price prediction using machine learning.

In this paper, we attempt to predict the Bitcoin price accurately taking into consideration various parameters that affect the Bitcoin value. For the first phase of our investigation, we aim to understand and identify daily trends in the Bitcoin market while gaining insight into optimal features surrounding Bitcoin price. Our data set consists of various features relating to the Bitcoin price and payment network over the course of five years, recorded daily. For the second phase of our investigation, using the available information, we will predict the sign of the daily price change with highest possible accuracy.

2. Evolution of bitcoin and security risk in bitcoin wallets.

This paper identifies trust factor and rewarding nature of bitcoin system, and analyze bitcoin features which may facilitate bitcoin to emerge as a universal currency. Paper presents the gap between proposed theoretical-architecture and current practical-implementation of bitcoin system in terms of achieving decentralization, anonymity of users, and consensus. Paper presents three different ways in which a user can manage bitcoins. We attempt to identify the security risk and feasible attacks on these configurations of bitcoin management. We have shown that not all bitcoin wallets are safe against all possible types of attacks. Bitcoin core is only safest mode of operating bitcoin till date as it is secure against all feasible attacks, and is vulnerable only against block-chain rewriting.

3. **Theeconomics of Bitcoin mining or Bitcoin in the presence of adversaries.**

The Bitcoin digital currency depends for its correctness and stability on a combination of cryptography, distributed algorithms, and incentive driven behaviour. We examine Bitcoin as a consensus game and determine that it relies on separate consensus.

4.Two Bitcoins at the Price of One Double-Spending Attacks on Fast PaymentsinBitcoin.

Bitcoin is a decentralized payment system that is based on Proof-of-Work. Bitcoin is currently gaining popularity as a digital currency; several businesses are starting to accept Bitcoin transactions. An example case of the growing use of Bitcoin was recently reported in the media; here, Bitcoins were used as a form of fast payment in a local fast-food restaurant. In this paper, we analyze the security of using Bitcoin for fast payments, where the time between the exchange of currency and goods is short (i.e., in the order of few seconds). We focus on double spending attacks on fast payments and demonstrate that these attacks can be mounted at low cost on currently deployed versions of Bitcoin.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009028 |

We further show that the measures recommended by Bitcoin developers for the use of Bitcoin in fast transactions are not always effective in resisting double-spending; we show that if those recommendations are integrated in future Bitcoin implementations, double-spending attacks on Bitcoin will still be possible. Finally, we leverage on our findings and propose a lightweight countermeasure that enables the detection of double spending attacks in fast transactions.

5. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies.

Besides attracting a billion dollar economy, Bitcoin revolutionized the field of digital currencies and influenced many adjacent areas. This also induced significant scientific interest. In this survey, we unroll and structure the manyfold results and research directions. We start by introducing the Bitcoin protocol and its building blocks. From there we continue to explore the design space by discussing existing contributions and results. In the process, we deduce the fundamental structures and insights at the core of the Bitcoin protocol and its applications. As we show and discuss, many key ideas are likewise applicable in various other fields, so that their impact reaches far beyond Bitcoin itself.

6. Bitcoin mining acceleration and performance quantification.

Since its introduction in 2009, Bitcoin, an open source, peer to peer, digital crypto currency has been growing in popularity and wide spread use. Growing attention, recognition by major financial institutions and high valued currency units (BTC) ascertains Bitcoin to a sturdy and ever increasing choice of currency. A public transaction log called the "Blockchain" keeps records of all committed transactions and Bitcoin ownership details, that is, addresses derived by cryptographic keys. Bitcoin mining, a process which results in the generation of new Bitcoins, is performed by miner operators for reception of incentives in the form of Bitcoins. This mining process is essentially operations of SHA-256 hashing of values in search of a hash digest smaller than a specific value. Once this winning hash has been discovered, a new block to Blockchain is added and BTC incentives are furnished by the Bitcoin network to the miner. This paper discusses methods of performing Bitcoin mining on non-custom hardware which results in contextually faster mining by combined usage of computing elements within machines in mining networks, both illegal and legal.

7. A Survey on Bitcoin Cryptocurrency and its Mining.

Bitcoin is a peer-to-peer digital decentralized cryptocurrency created by an individual under pseudonym Satoshi Nakamoto. In fact, it is the first digital decentralized currency. The importance of digital cryptocurrency and the concept of blockchain have been explored by several developers and organizations. It is assumed to be one of the secure and easy payment methods that can be used in the coming days. In this paper, we survey various topics under Bitcoin such as blocks, blockchains, mining process and proof of work(PoW).

8. Analysis of Bitcoin Cryptocurrency and Its Mining Techniques

The mining of Bitcoin requires very high computation power. Since miners are solving the complex mathematical puzzle through hardware, they need to be fast in order to be the first solving the block. The miner who successfully solves the block gets rewarded with Bitcoin. Mining can be done by a single person, or it can be done by pool, where a bunch of miners combines in a network to mine a single block. Single mining, also referred to as solo mining is difficult since the difficulty of Bitcoin mining is increasing every day. Pool mining is another option for those who have fewer resources for mining. We propose an efficient way of mining Bitcoin by analyzing several results through self-experiment, online exchange market data, real-time Bitcoin block data, different mining pools' efficiency data and much more. Several factors are needed to be taken into consideration during mining because we may never mine a single Bitcoin even if we invest thousands of dollars on mining Bitcoin.

III. METHODOLOGY

Onlinewallets:

Your private keys are stored online, on a machine that is connected to the Internet and under another person's control, in web-based wallets. There are many such online services, some of which connect to desktop and mobile wallets and replicate your addresses across all the devices you own.

One benefit of web-based wallets is that you may access them from any location and on any device. However, they do have one significant flaw: if not done properly, they may hand control of your private keys to the company running the website, thereby putting your bitcoins out of your control.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009028 |

An integrated bitcoin exchange and wallet, Coinbase, runs its online wallet internationally. By using its exchange services, anyone in the US and Europe can purchase bitcoin. Users all throughout the world can store, transmit, receive, and purchase bitcoins using Circle. Your private address keys are encrypted by Blockchain before being sent to its servers; encryption is transmitted through the browser.

SHA-256:

The NIST (National Institute of Science and Technology) announced the Secure Hash Algorithm (SHA) family of cryptographic hash functions. The SHA-256 Hashing algorithm is utilized in the Bitcoin network. The 256-bit integer that is always produced by this algorithm is typically expressed using the hexadecimal number system. The hash of the input is the common name for the SHA-256 function's output. Four subgroups make up the SHA group: SHA-0, SHA-1, SHA-2, and SHA-3.

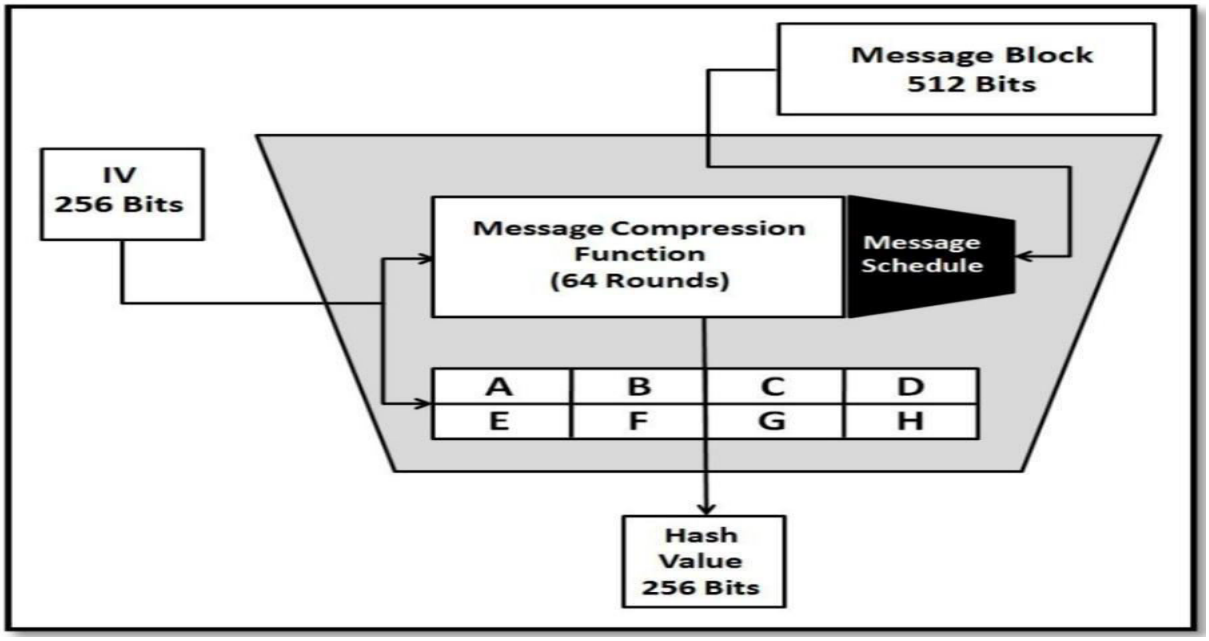


Figure 3. Cryptographic hash function

The process of adding transaction records to the Bitcoin public ledger is known as mining. The sender's signature is required for a transaction to be regarded as legitimate. Mining becomes increasingly challenging as more miners join the network.

A block is verified and added to the blockchain network using the modified Bitcoin protocol in an average of 10 minutes. A block is regarded as valid if it has Proof of Work. The miner who successfully extracts a block is rewarded. As payment for their efforts in verifying the block, the miners receive Bitcoin (12.5 Bitcoin per block at the time of writing). Along with the prize, they also get the transaction fee from every transaction in the block. The miners are encouraged to mine Bitcoin via this reward system. Figure 17 illustrates how the Bitcoin blockchain operates in general.

Proof of Work(Pow)

Bitcoin invented the Pow consensus algorithm, which is now widely utilized by many other cryptocurrencies. It comprises of a challenging mathematical cryptographic challenge. It searches for a value known as nonce (number only used once). The nonce is a counter that is used in the block header and is what the miners alter to change a block's hash value so that it satisfies the hash requirements. When using SHA-256 to hash a value, the output has always started with a specific number of zeros.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009028 |

The average effort needed for a specific block is determined by the exponential to the number of zeros in the right hash. This indicates that a substantial amount of computation went into the verification process as shown by the Proof of Work. This high level of computing is made possible by the equipment that miners employ. The block is mined by the

miners by computing its hash using a changing nonce. To change the nonce, there is no set formula or pattern. It varies in an arbitrary order. The miner adjusts the nonce until the calculated hash value is equal to or less than the specified goal value.

The process of adding transaction records to the Bitcoin public ledger is known as mining. The sender's signature is required for a transaction to be regarded as legitimate. Mining becomes increasingly challenging as more miners join the network.

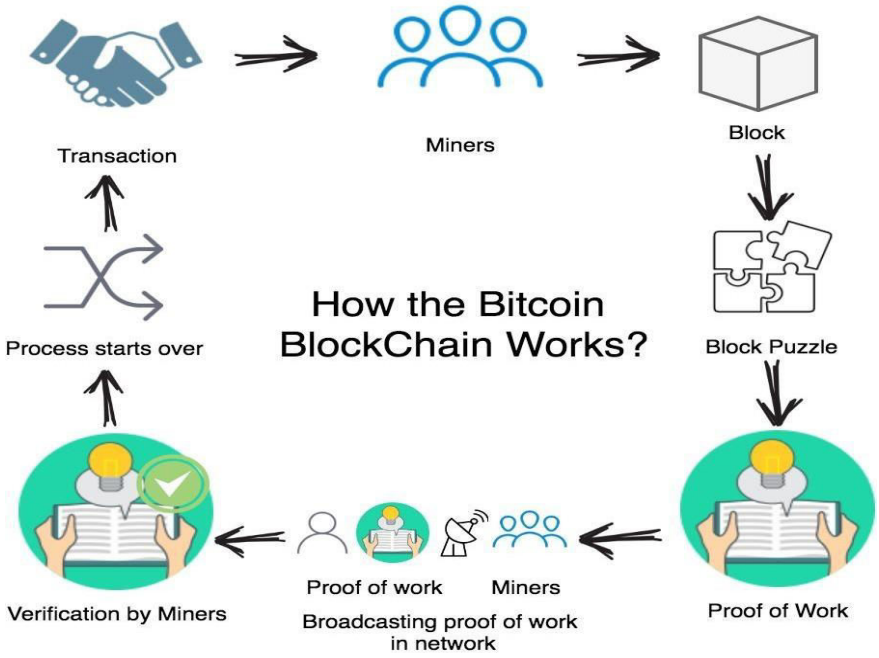


Figure4: Working mechanism of bitcoin blockchain

A block is verified and added to the blockchain network using the modified Bitcoin protocol in an average of 10 minutes. A block is regarded as valid if it has Proof of Work. The miner who successfully extracts a block is rewarded. As payment for their efforts in verifying the block, the miners receive Bitcoin (12.5 Bitcoin per block at the time of writing). Along with the prize, they also get the transaction fee from every transaction in the block. The miners are encouraged to mine Bitcoin via this reward system. Figure 17 illustrates how the Bitcoin blockchain operates in general.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 9, September 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1009028 |

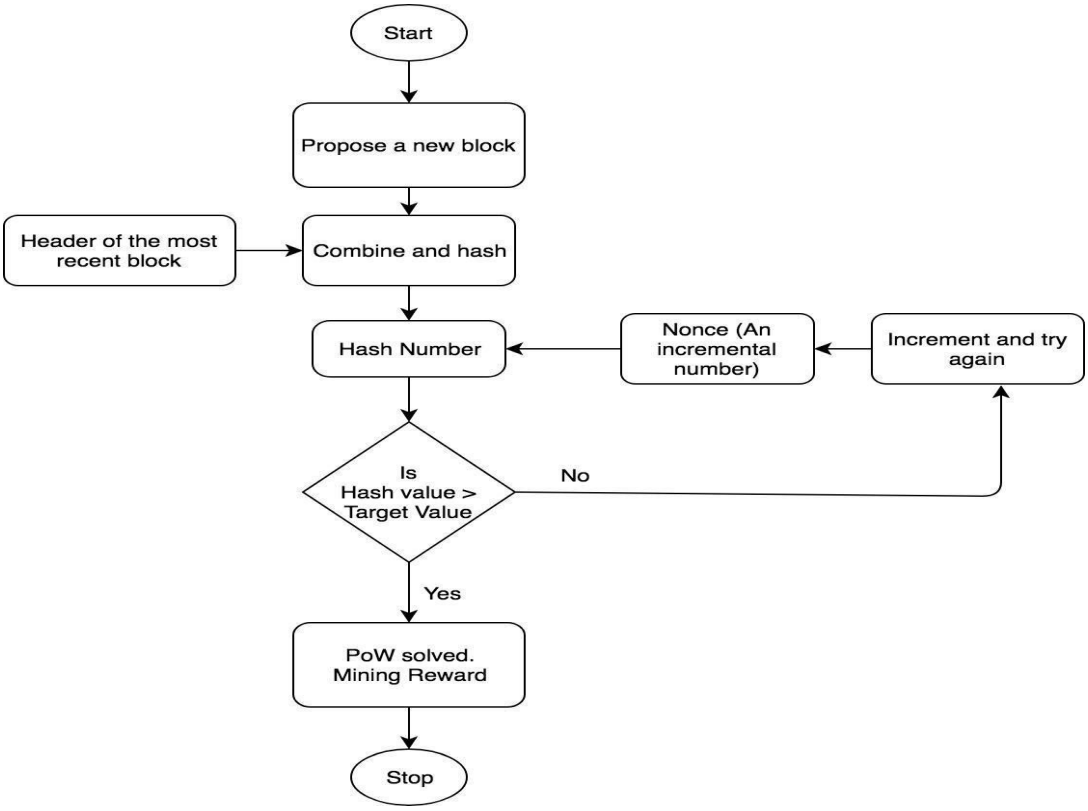


Figure5: Flowchart of a Bitcoin mining process

IV. CONCLUSION AND FUTURE WORK

Bitcoin mining is the process of adding transaction records to Bitcoin's public ledger of past transactions or blockchain. This ledger of past transactions is called the block chain as it is a chain of blocks. The block chain serves to confirm transactions to the rest of the network as having taken place. Bitcoin nodes use the block chain to distinguish legitimate Bitcoin transactions from attempts to re-spend coins that have already been spent elsewhere.

In this paper, we studied the analysis of Bitcoin Mining in various aspects. Bitcoin is being used as an alternative to fiat currencies. Since Bitcoin is decentralized and works on the concept of the blockchain, all the transactions are transparent and fair. Mining a Bitcoin consumes a lot of power. Countries like Venezuela, Myanmar. Kuwait, Ukraine, Uzbekistan, India, etc. would be the best solution for miners and mining pool. Due to the limitation of hardware resources, we could not mine the Bitcoin on our own. The future work for this thesis would be either buying some good hardware by securing funding or collaborating with mining pools to use their hardware for a research purpose.

REFERENCES

1. Bitcoin price prediction using machine learning.
2. Evolution of bitcoin and security risk in bitcoin wallets.
3. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries
4. Two Bitcoins at the Price of One Double-Spending Attacks on Fast PaymentsinBitcoin.
5. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies.
6. Bitcoin mining acceleration and performance quantification.
7. A Survey on Bitcoin Cryptocurrency and its Mining.
8. Analysis of Bitcoin Cryptocurrency and Its Mining Techniques.
6.https://www.bitdegree.org/crypto/tutorials/how-to-mine-bitcoin
7.https://www.geeksforgeeks.org/how-does-bitcoin-mining-work/

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details