IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 10, October 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 10, October 2022||

| DOI:10.15680/IJIRSET.2022.1110019 |

# BTC Mining and Bitcoin Transactions in Blockchain Network

**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 is a digital cryptocurrency that has generated considerable public interest, including both booms in value and busts of exchanges dealing in Bitcoins. One of the fundamental concepts of Bitcoin is that work, called mining, must be done in checking all monetary transactions, which in turn creates Bitcoins as a reward. In this paper we look at the energy consumption of Bitcoin mining. We consider if and when Bitcoin mining has been profitable compared to the energy cost of performing the mining, and conclude that specialist hardware is usually required to make Bitcoin mining profitable. We also show that the power currently used for Bitcoin mining is comparable to Ireland's electricity consumption.

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

## I. INTRODUCTION

**What is Blockchain?**

A blockchain is a constantly growing ledger which keeps a permanent record of all the transactions that have taken place in a secure, chronological, and immutable way.Figure 1. shows the hash function in blockchain.

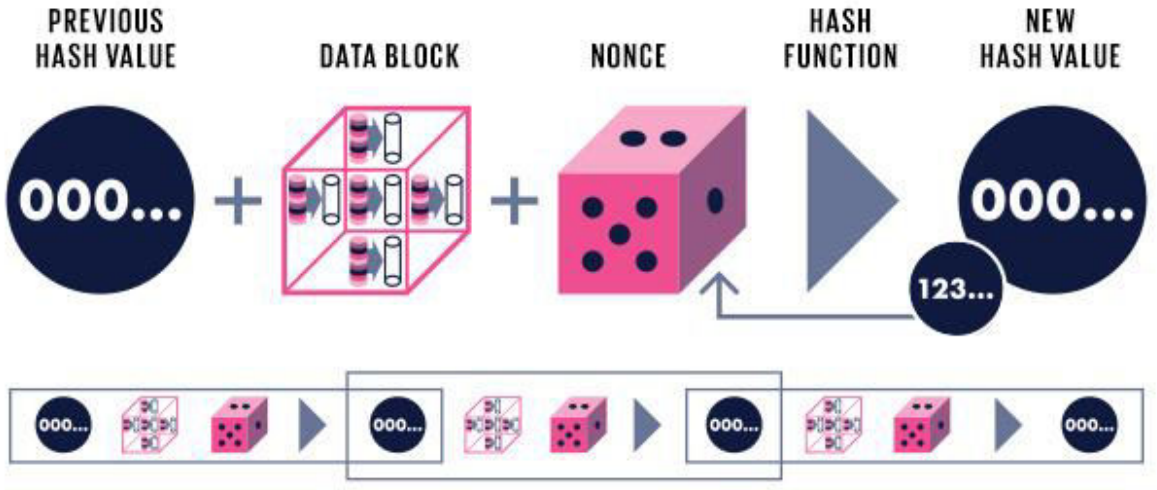


**Figure 1**.Cryptography in blockchain using Hash function.

Let's breakdown the definition,

**Ledger:** It is a file that is constantly growing.

**Permanent:** It means once the transaction goes inside a blockchain, you can put up it permanently in the ledger.

**Secure:** Blockchain placed information in a secure way. It uses very advanced cryptography to make sure that the information is locked inside the blockchain.

**Chronological:** Chronological means every transaction happens after the previous one.

**Immutable:** It means as you build all the transaction onto the blockchain, this ledger can never be changed.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 10, October 2022||

| DOI:10.15680/IJIRSET.2022.1110019 |

A blockchain is a chain of blocks which contain information. Each block records all of the recent transactions, and once completed goes into the blockchain as a permanent database. Each time a block gets completed; a new block is generated.

## II. NEED OF BLOCKCHAIN

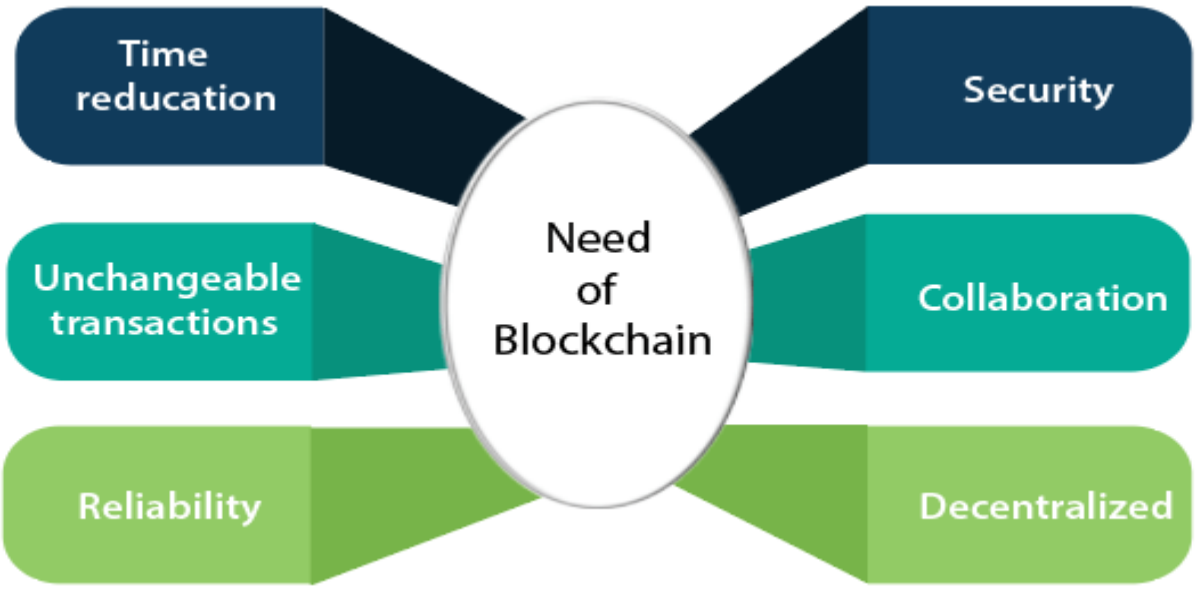


**Figure 2.** Uses of Blockchain technology.

**Blockchain technology has become popular because of the following.**

- **Time reduction:** In the financial industry, blockchain can allow the quicker settlement of trades. It does not take a lengthy process for verification, settlement, and clearance. It is because of a single version of agreed-upon data available between all stakeholders.
- **Unchangeable transactions:** Blockchain register transactions in a chronological order which certifies the unalterability of all operations, means when a new block is added to the chain of ledgers, it cannot be removed or modified.
- **Reliability:** Blockchain certifies and verifies the identities of each interested parties. This removes double records, reducing rates and accelerates transactions.
- **Security:** Blockchain uses very advanced cryptography to make sure that the information is locked inside the blockchain. It uses Distributed Ledger Technology where each party holds a copy of the original chain, so the system remains operative, even the large number of other nodes fall.
- **Collaboration:** It allows each party to transact directly with each other without requiring a third-party intermediary.
- **Decentralized:** It is decentralized because there is no central authority supervising anything. There are standards rules on how every node exchanges the blockchain information. This method ensures that all transactions are validated, and all valid transactions are added one by one.

**Bitcoin**

Bitcoin is an innovative payment network and a new kind of money.Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network. Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part. Through many of its unique properties, Bitcoin allows exciting uses that could not be covered by any previous payment system.

Bitcoin (₿) is a decentralized digital currency that can be transferred on the peer-to-peer bitcoin network.[7] Bitcoin transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a blockchain. The cryptocurrency was invented in 2008 by an unknown person or group of people using the

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 10, October 2022||

| DOI:10.15680/IJIRSET.2022.1110019 |

name Satoshi Nakamoto.[10] The currency began use in 2009,[11] when its implementation was released as open-source software.

## III. METHODOLOGY

**Bitcoin mining**

**What Is Bitcoin Mining?**

Bitcoin mining is the process of creating new bitcoin by solving puzzles. It consists of computing systems equipped with specialized chips competing to solve mathematical puzzles. The first bitcoin miner (as these systems are called) to solve the puzzle is rewarded with bitcoin. The mining process also confirms transactions on the cryptocurrency's network and makes them trustworthy.

**Processofmining**

It is a must to join the Bitcoin network and establish connections with other nodes in order to mine bitcoins. The primary six duties that miners must complete are listed below.

1.Miners must keep an eye out for broadcast transactions on the network. They must validate the transactions by ensuring that the signatures are accurate and that the outputs have not already been used. To lessen the issue of double spending, this is done.

2. Miners must own all of the prior blocks that make up the blockchain before entering the network.
They keep an ear out for any fresh blocks that the network broadcasts. They must then validate each transaction in each block that they receive in order to determine its validity. They must also determine whether the clock has a valid nonce.

3. Miners can start creating their own blocks once they get the most recent version of the blockchain. In order to accomplish this, the miner groups newly received transactions into a new block that extends the most recent block.

4. The block must now contain a nonce in order for mining to continue. One of the difficult but essential mining steps is this one.

5. Assume that the block is approved upon the discovery of a nonce. Even if the block is accepted, there is no assurance that it will be included in the consensus chain. The block will become a link in the consensus chain if additional miners accept the same block and begin mining on top of it.

6. The miner who worked on locating the nonce for that specific block would be rewarded if all the miners accepted the block and contributed to the consensus chain. The current block reward is 12.5 Bitcoins. Additionally, the miner also receives any transaction fees that were paid as part of any transactions that were included in the block.

**I. Method of payment for cryptocurrency**

This technique enables older users or adult gamers to pay real money or an equivalent cryptocurrency using real money systems like prepaid and credit cards or online payment systems like PayPal. Each platform for digital currencies has a unique pricing range and exchange rate that correspond to the amount of money spent. On the site, substantial sums of money are acquired from consumer accounts.

**Figure 3.**displays the user page after successful loging with two-factor authentication using a password and OTP.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 10, October 2022||

| DOI:10.15680/IJIRSET.2022.1110019 |

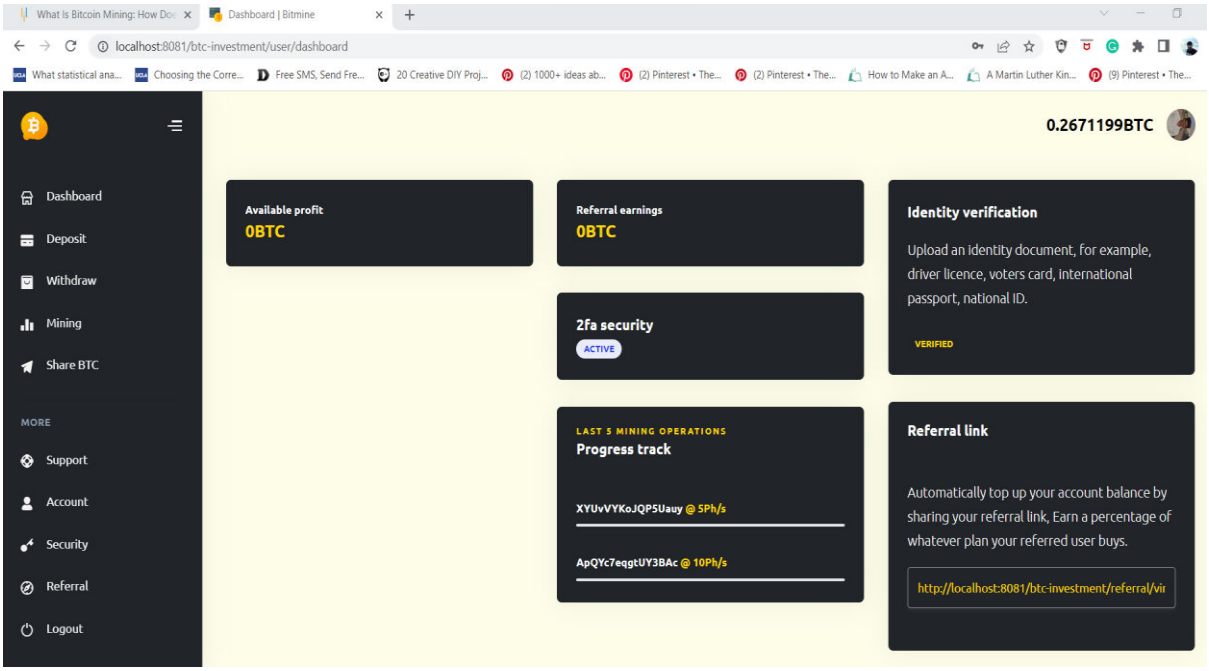


**Figure 3**. User page

## II. Method based on an offer:

The majority of online players lack the resources or know-how to exchange cash for cryptocurrencies. Seeing promotional advertising, completing surveys, earning gaming prizes, and signing up for a free trial subscription are all ways that users and gamers, young and old, can earn bitcoin. This method is thought to be the quickest way to generate cryptocurrency.

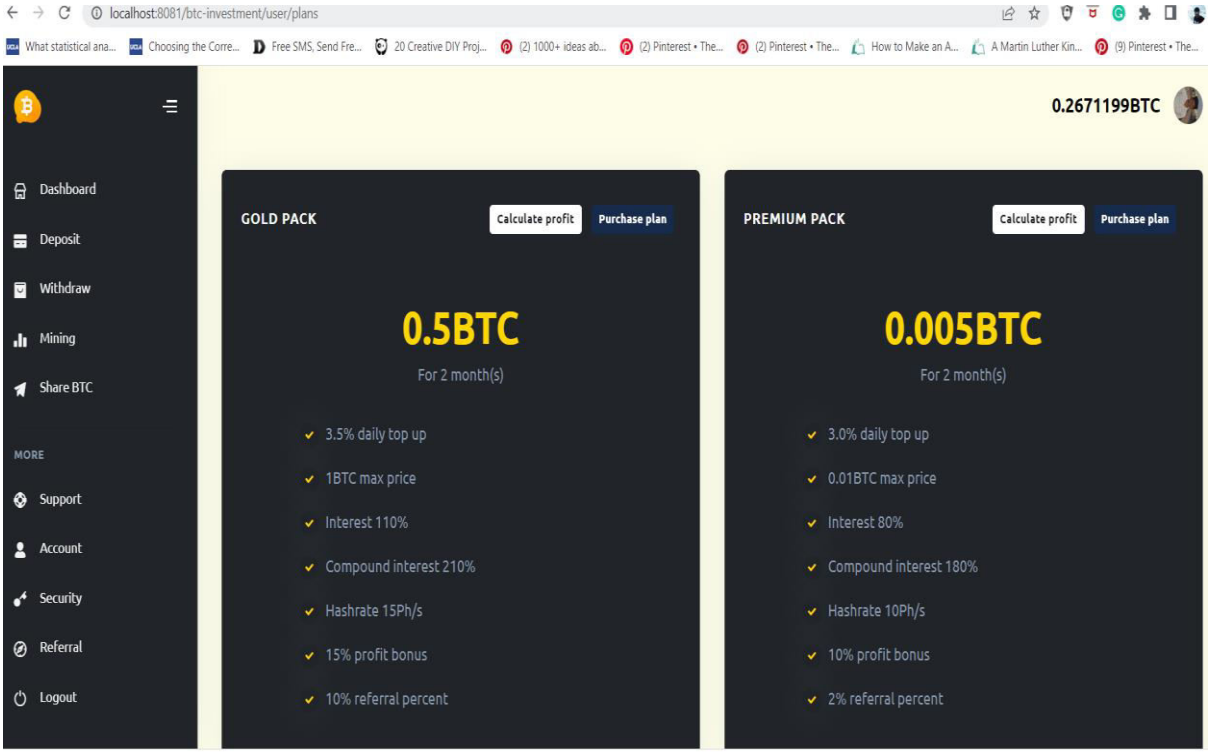


**Figure 4.** Bitcoin mining plans

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 10, October 2022||

| DOI:10.15680/IJIRSET.2022.1110019 |

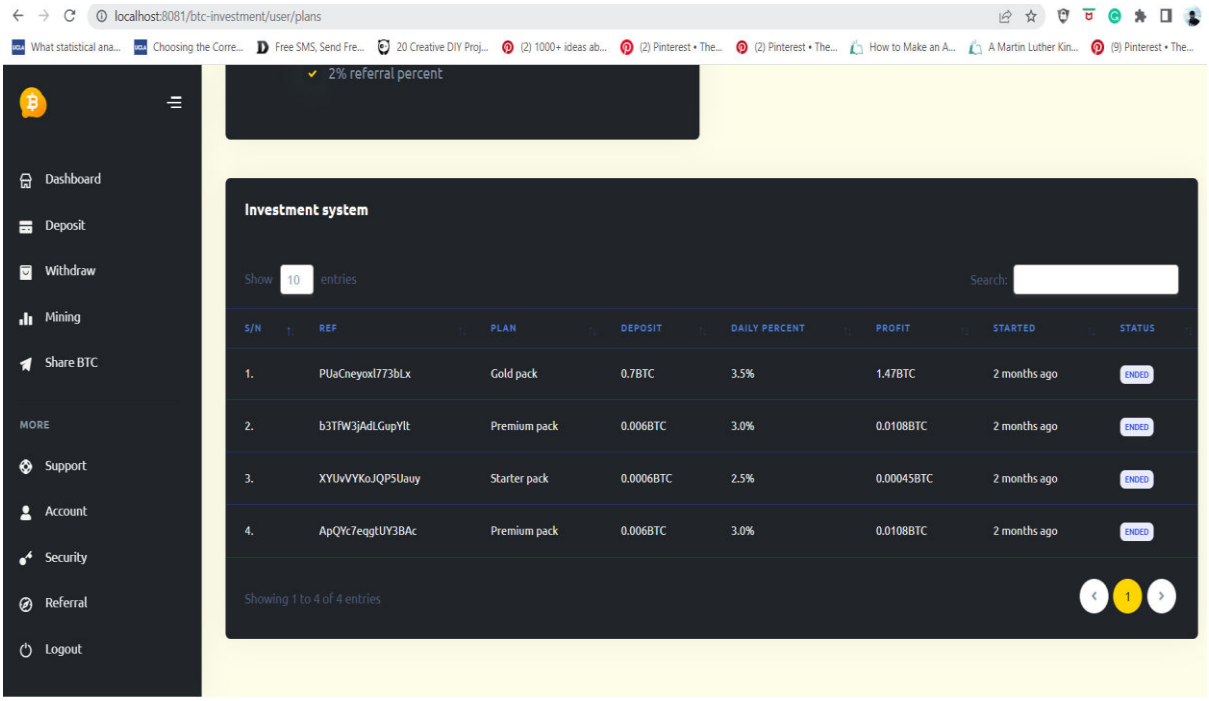


**Figure 5.** History of Plans and profit

## III. Cryptocurrency spending and exchange:

The conversion of digital currency for physical items and the conversion of digital currency for actual goods like money, goods, and services are the two categories under which crypto is melted and exchanged. This paper contains some challenges and problems.We can also share BTC like similar to PhonePe,Google Pay.Figure 6. showing history of shared BTC.

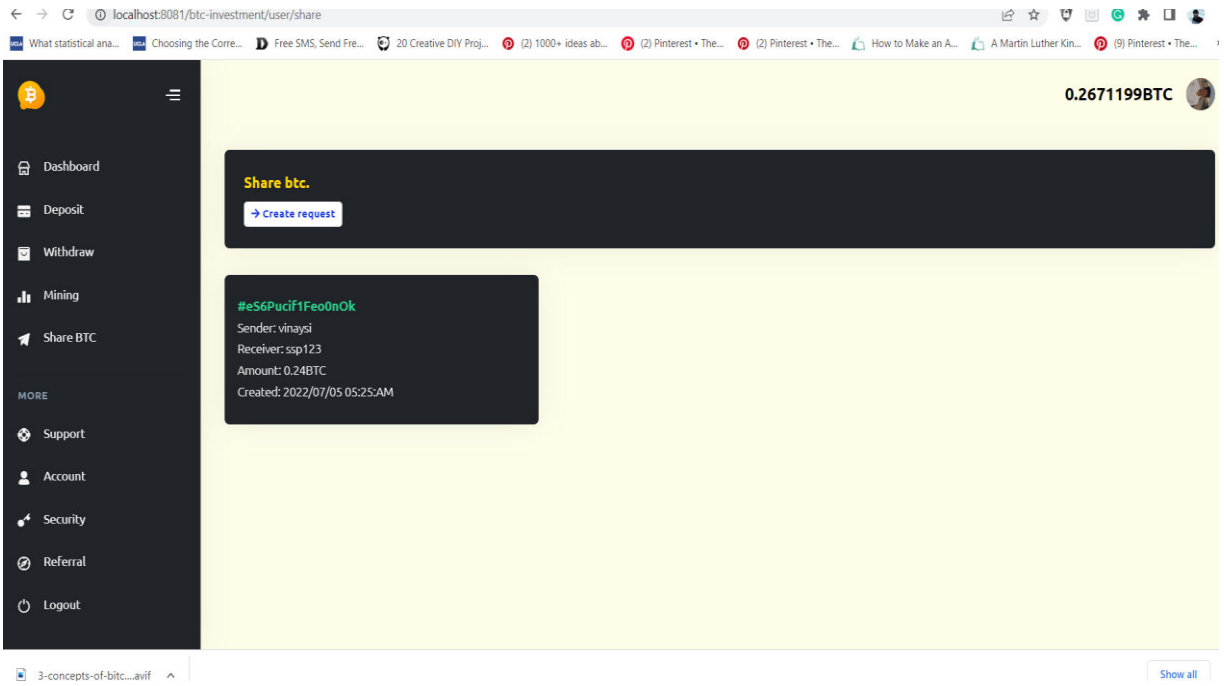


**Figure 6.** Sharing BTC

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 10, October 2022||

| DOI:10.15680/IJIRSET.2022.1110019 |

## IV. CONCLUDE

Bitcoin is basically a digital currency that is currently used as a form of payment. Bitcoin is a cryptocurrency and the transactions related to bitcoins take place in the blockchain network. Every bitcoin is stored in a virtual wallet and transaction involves the transfer of bitcoin from one wallet to another. Bitcoins can be sent from peer to peer irrespective of geographical location without any intermediator in between (for example bank per se). it works in a decentralized way, meaning nobody can interfere with your digital money, only you are responsible for your bitcoins.

Bitcoin mining is very important**.** It's worth doing even if you're not making huge (or any) profits. The more miners working on the network, the more secure it is**.** Some hobbyist miners mine the network at a loss. They see it as their duty to run a miner to increase the network's decentralization and reduce the likelihood of a potential attack being successful**.**

Unfortunately, Bitcoin mining is highly competitive these days. Without a huge investment and the freedom to set up somewhere with low electricity rates and a cool climate, your chances of making a lot of money Bitcoin mining are very slim.

## REFERENCES

1.AnalysisofBitcoinCryptocurrencyandItsMiningTechniques
2.Bitcoin price prediction using machine learning.
3.Evolution of bitcoin and security risk in bitcoin wallets.
4. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries
5. Two Bitcoins at the Price of One Double-Spending Attacks on Fast Payments in Bitcoin.
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: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com



Scan to save the contact details