BITCOIN

Seminar Report

Submitted In Partial Fulfilment of the Requirements For The

Degree of

MASTER OF COMPUTER APPLICATION

Department of

Mathematical and Computational Sciences

NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA

SURATHKAL, MANGALORE – 575025

Submitted By:

Name: RAVI JOHN MARK HORO

Roll No.: 174CA054

MCA 2ND SEMESTER

Submitted To:

Dr. Vishwanath K P

Mr. Balakrishna

DECLARATION

I hereby declare that the seminar report entitled "**BITCOIN**" which is being submitted to the National Institute of Technology Karnataka, Surathkal, in partial fulfilment of the requirements for mandatory learning course of Master of Computer Applications in the Department of Mathematical and Computational Sciences, is a bonafide report of the work prepared by me. This material is collected from various sources with atmost care and is based on facts and truth.

Name: RAVI JOHN MARK HORO

Roll No. : 174CA054

Class: MCA 2ND SEM

Place: NITK, SURATHKAL

CERTIFICATE

This is to certify that the P.G. Seminar Report entitled "**BITCOIN**" submitted by **RAVI JOHN MARK HORO (ROLL NO. 174C054)** as the record of the work carried out by them is accepted as the P.G. Seminar Work Report submission in partial fulfilment of the requirements for mandatory learning course of Master of Computer Application in the Department of Mathematical and Computational Sciences.

CONTENTS

1. INTRODUCTION

At the most basic level, Bitcoin is no different than the money in our wallets. Just like money, it can be used to buy goods or products. A person holds bitcoins in a Bitcoin wallet - in a mobile app or in computer - and can send and receive bitcoins through it.

However, this is just from the user's perspective. Bitcoin is essentially a consensus network that enables a new payment system and a completely new digital money. Digital money means that Bitcoin does not have a physical existence. It exists only electronically. It was created in 2009 by someone using the pseudonym “Satoshi Nakamoto”. It is the first decentralized peer-to-peer payment network i.e. it can be sent from user to user without having to pass through an intermediary like a bank. Also, Bitcoin isn't attached to a bank or a government. So it doesn't have a central issuing authority. Basically, it means that there is no organization deciding when to make more bitcoins, figuring out how many to produce and keeping track of the coins. Bitcoin is also known as a cryptocurrency, as it uses cryptography to secure the transactions.

Bitcoins are created as a reward for something known as “mining”. They can be exchanged for other currencies, products and services. Bitcoin transactions are very fast, secure, can be sent to anyone without any intermediaries, and provide anonymity to the users. However Bitcoins are highly volatile. Their value increases/decreases at a very high rate. By the end of 2017, 1 Bitcoin was equal to around 19,000 USD. However, it started declining and in 2018, 1 Bitcoin is equal to around 11,000 USD. Therefore, investment in Bitcoin is highly risky.

2. HISTORY OF BITCOIN

Bitcoin is the first implementation of a concept called "cryptocurrency", suggesting the idea of a new form of money that uses cryptography to control its creation and transactions rather than a central authority.

On 18 August 2008, the domain name bitcoin.org was registered. Later that year on 31 October, a link to the paper authored under the pseudonym Satoshi Nakamoto title "Bitcoin: A Peer-to-Peer Electronic Cash System" was posted to a crypotgraphic mailing list. This paper detailed methods of using a peer-to-peer network to generate what was described as "a system for electronic transactions without relying on trust". In January 2009, the bitcoin network came into existence with the release of the first open source bitcoin client and the issuance of the first bitcoins, with Satoshi mining the first block of bitcoins ever(known as the genesis block), which had a reward of 50 bitcoins. Hal Finney, one of the first supporters, downloaded the bitcoin software the day it was released, and received 10 bitcoins from Satoshi in the world's first bitcoin transaction.

Before disappearing from any involvement in bitcoin in 2010, Satoshi Nakamoto, without revealing much about himself, handed over the reins of Bitcoin to developer Gary Andresen, who then became a lead developer at the "Bitcoin Foundation" which is a bitcoin community who looks after the development of bitcoin network.

3. BASIC TERMINOLOGIES

3.1 Wallet

A Bitcoin wallet is like a wallet to store Bitcoins. It is a program to send and receive Bitcoins and monitor Bitcoin balances. When an account is created, the wallet is linked to two unique mathematically related keys known as "Private and Public Keys". Private key as the name specifies should be kept a secret and safe as Bitcoins are sent by signing using private keys while the public key is used to receive Bitcoins as it is the users' address. Even though the two keys are related, thers's no way to figure out the private key from the public key.

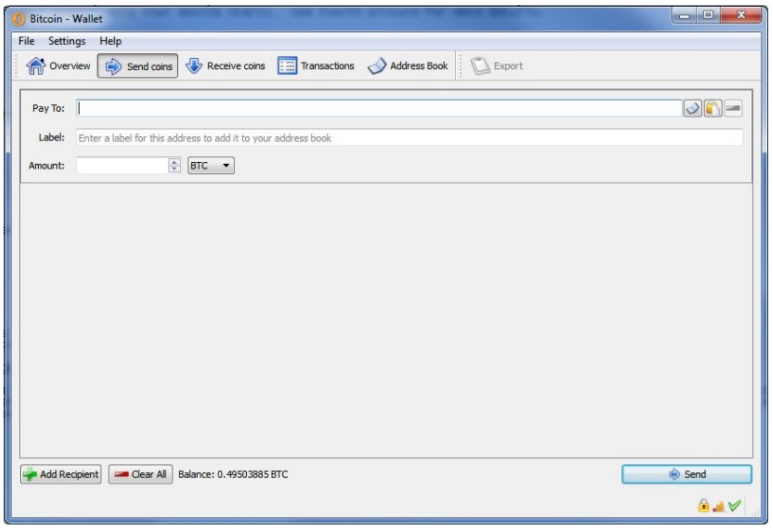

Fig.3.1 Bitcoin Wallet

3.2 Transaction

A transaction is a transfer of Bitcoin value from a sender to the receiver. It is broadcasted to the network. A transaction is then validated i.e. it is checked if the sender has enough Bitcoins to send. If found valid, the transaction is added to the block. If not, it is discarded.

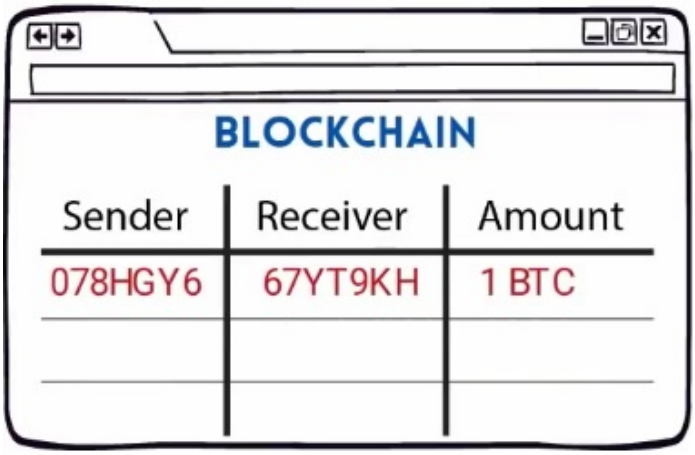

Fig.3.2 Transaction recorded in blockchain

3.3 Block

A block is basically a collection of some or all of the most recent Bitcoin transactions that have not been entered in any previous block. On an average, a block contains approximately 1000 – 2000 transactions.

Contents of a block:

- **Transactions**
  A block contains a number of recent Bitcoin transactions

- **Hash**
  A block is identified by something known as a "hash". A hash is generated by a "hash function" which reduces any amount of input text or data to a 64-character string. The hash function that bitcoin uses is SHA256, which stands for Secure Hash Algorithm 256-bit. Every block has a unique hash. It can be considered as a fingerprint.

Fig.3.3 Hash of a block

- **Hash of previous block**
  A block also contains hash of the previous block through which a block is connected to the previous block, forming a chain like structure.

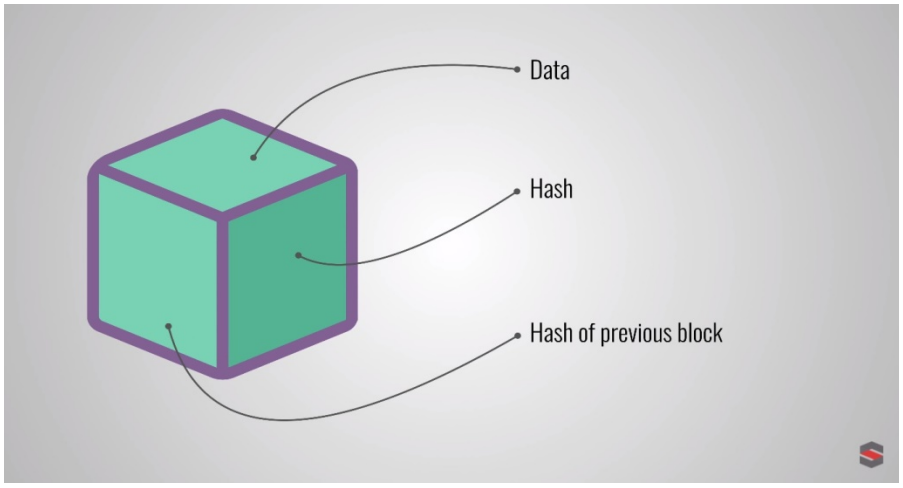

Fig.3.4 Contents of a Block

3.4 Blockchain

Blockchain, as the name implies, is a chain of blocks. It is a huge global ledger which records every transaction that has ever happened. Blockchain is maintained by people in the Bitcoin network. Anybody can volunteer to keep the blockchain up to date. The data is kept in sync i.e. everyone on the network has the same copy of the blockchain. As of 2018, the size of blockchain data is 149 GB.

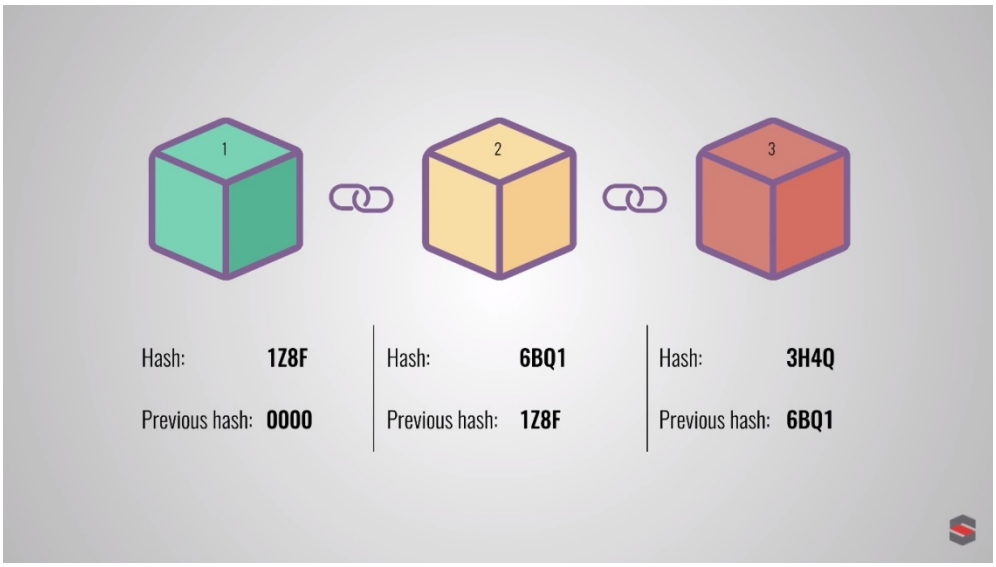

Fig.3.5 Blockchain of Three Blocks

3.5 Miners

Miners are the people in the Bitcoin network who maintain the blockchain. They use specially designed computers to calculate the hash of the block and add the block to the blockchain. Every time a block is added to the blockchain, 12.5 bitcoins (as of now) are awarded to the first miner who gets to add the block. In addition to the reward, miners may also be tipped a very small amount for each transaction they add to the ledger.

3.6 Mining

Mining is the process of calculating hash of the block. For this, what the miners have to do is to calculate a hash lesser than the target hash, which is set by the Bitcoin Network. On an average, it takes about 10 minutes. Whoever calculates the hash first, gets to add the block in the blockchain. After the hash is calculated, it is included in the block and then the block is added to the blockchain.

4. WORKING OF BITCOIN

When sending Bitcoins to someone, the transaction detail i.e. how many Bitcoins to send and to whom, is encrypted using the private key, also known as "signing", and sent to the Bitcoin network. This transaction is then validated. There is a check built into the Bitcoin system. Both the Bitcoin network and wallet automatically checks the previous transactions to make sure that there is enough Bitcoins to send in the first place by checking the senders' transaction history. The system can do so as it has the senders' public key(address) and all transactions are public on the Bitcoin ledger.

If the transaction is invalid, it gets rejected. If the transaction is valid, it gets included into a "block" along with a bunch of other transactions.

When a block is created, its hash is being calculated. This is done by people known as "miners" with the help of computers. Whoever calculates the hash first, gets to add the block to the blockchain. This calculation can take seconds or much later. However, the difficulty is kept at a level such that on an average, it is expected to take 10 minutes. After the block is added by a miner, it is announced on the network so others can verify that the block fulfils the criteria. If the block is found invalid, it is rejected by the network. If not, it stays in the blockchain. The receiver, then, receives the Bitcoins. And miners start working on the next block.

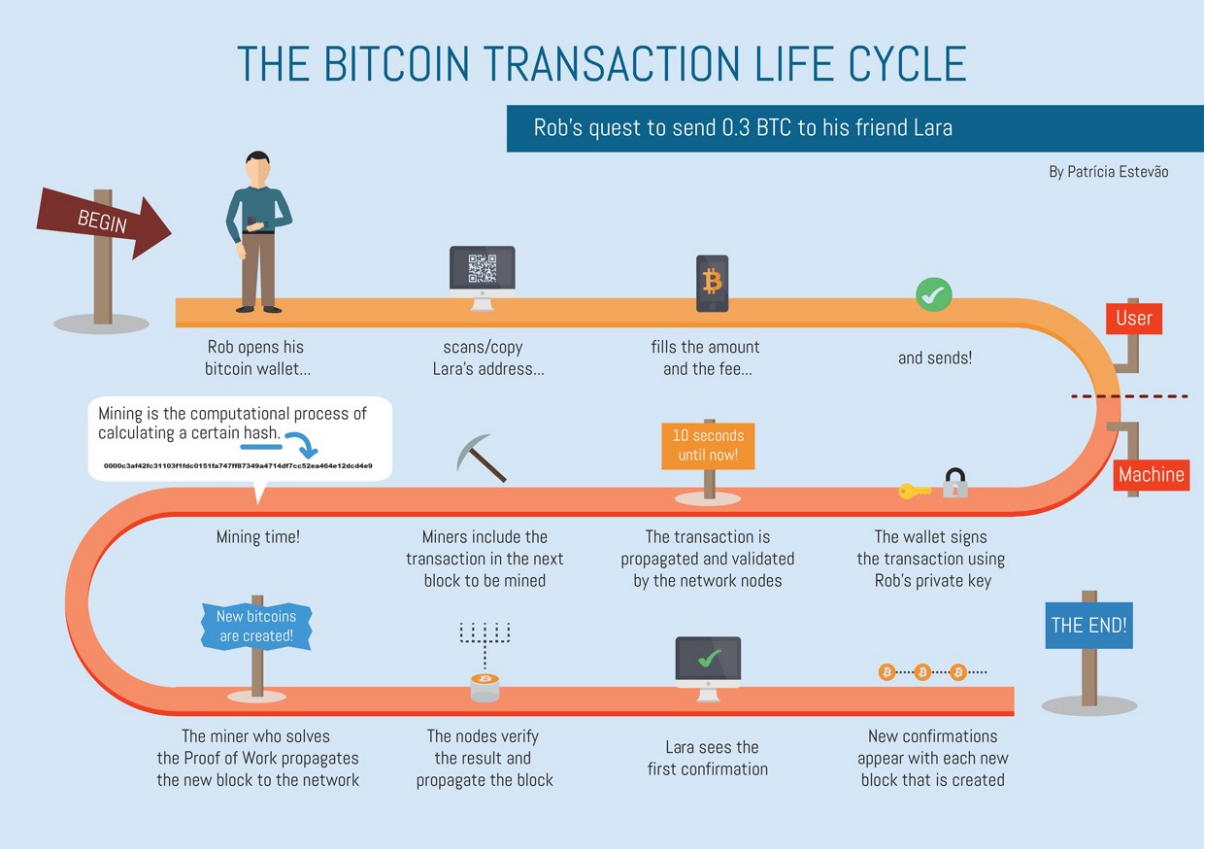

Fig.4.1 Bitcoin Transaction

5. HARDWARE FOR BITCOIN MINING

Bitcoin mining has evolved rapidly over the last 7 years, with three distinct generation of miners in terms of power efficiency:

5.1 CPUs (2009-2010)

In the early days, Bitcoin mining was nothing more than a lucrative hobby for nerdy cryptocurrency enthusiasts. The only hardware required, in the beginning, was a simple computer with a decent CPU. Although these computers did not consume more electricity, they were slow.

Fig.5.1 CPUs used for mining in the early days

5.2 GPUs and FPGAs (2010-2013)

Soon miners discovered that high end graphics card used for gaming were far more effective in mining Bitcoins. The use of GPUs increased the mining power by as much as 100x while consuming a lot of electricity and generating a lot of heat.

Next came FPGAs or Field Programmable Gate Array. The improvement here being in the power usage rather than actual mining speed, power consumption fell by as much as 5x.

Fig.5.2 GPU for mining

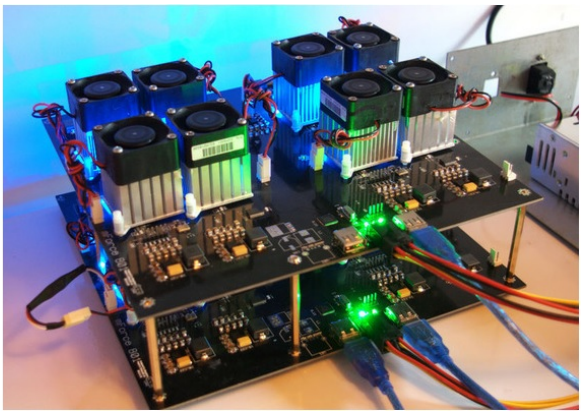

Fig.5.3 FPGA with 8 cores

5.3 ASICs (2013-present)

Then came ASICs or Application Specific Integrated Circuits. ASICs are designed for the sole purpose of mining, with no other functional capabilities. It increased the mining power by as much as 100x more, while also using significantly less power than had been the case with CPUs, GPUs and FPGAs.

Fig.5.4 An ASIC

6. ACQUIRING AND SPENDING BITCOINS

6.1 Ways to acquire Bitcoin

6.1.1 Mine your own Bitcoins

It is the only way to get new Bitcoins which are not in circulation. Bitcoin mining is a process in which new Bitcoins are generated. However, mining is not an easy task and requires huge computational power. Mining is also very costly and time consuming process.

6.1.2 Accept Bitcoin for a product or service

Mining is not possible for all. However, another way to earn Bitcoins is to accept Bitcoins as a payment for products or services sold or getting paid for a job in Bitcoins.

6.1.3 Buy Bitcoins

Another way to get bitcoins is by purchasing bitcoins online or offline at current exchange rate from a Bitcoin exchange.

6.2 Ways to use Bitcoin

6.2.1 Using it as money

Starting to use Bitcoins can be exciting because it is a new technology. Bitcoins can be used to purchase just about everything you want. Over 100,000 merchants worldwide accept Bitcoins as payment. So purchasing from them is an option. Also search engines like "Spendabit", shows millions of products, all available for purchase with bitcoins.

Also Bitcoins are divisible. They can be divided down to 8 decimal places. Therefore, 0.00000001 BTC is the smallest amount that can be handled in a transaction. Hence, Bitcoin can be divided for use in smaller transactions.

6.2.2 Converting it to cash

Bitcoin exchanges allow users to exchange Bitcoin units for currencies at variable exchange rates. Most Bitcoin exchanges typically take less than 1% of each transaction value.

7. BITCOINS IN CIRCULATION

Every single bitcoin that exists was created to reward a bitcoin miner. As of 2018, 80% i.e. approximately 16,800,000 bitcoins have been mined and 20% is left for miners to acquire. It's also worth noting that every 210,000 blocks or about every 4 years, the number of coins generated when a new block is added to the blockchain, goes down by half. So what started as a reward of 50 bitcoins in 2009, decreased to 25 and then to 12.5 bitcoins and will keep on decreasing. According to current projections, the last bitcoin - probably around 21 millionth coin - will be mined in the year 2140, unless a change to the protocol is made to increase the supply.

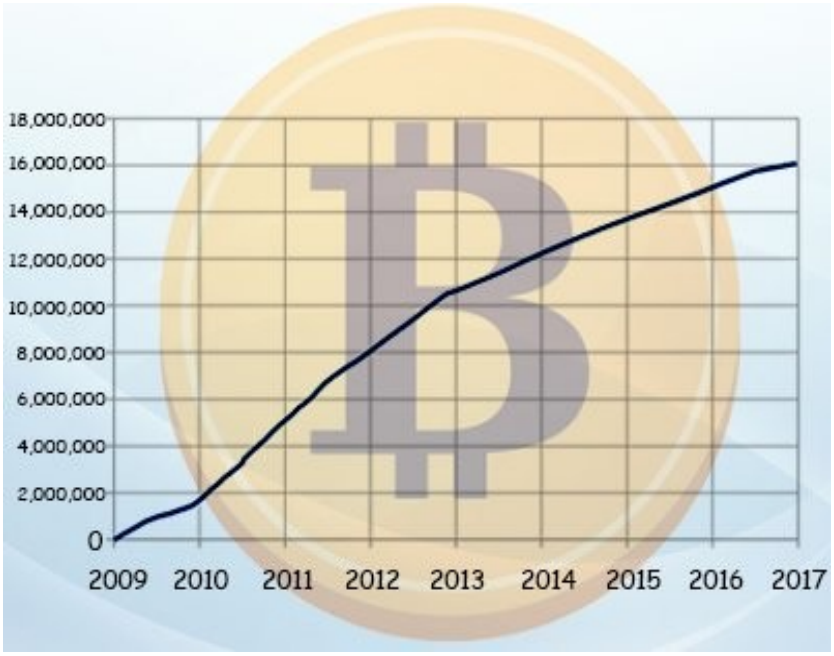

Fig.7.1 Bitcoins in circulation

8. ADVANTAGES OF BITCOIN

8.1 Anonymous and Private

Bitcoin transactions are completely anonymous and private. Unlike in payments through bank, where the transactions can be tracked and identified, bitcoin transactions cannot be identified. A person can only know the addresses of bitcoins on which the payment has been sent and received. But to whom these addresses belong cannot be identified.

8.2 Payment Freedom

Paying through bitcoins provide us the utmost freedom. Bitcoins can be sent to any person in any part of the world. No intermediaries in between. No bank holidays/strikes. No boundaries or borders. No payment limit.

8.3 Low/Minimal Fees

Bitcoin transactions are currently processed with either no fees or extremely small fees, which is lesser compared to what is charged by banks.

.

8.4 It's fast

Bitcoin transactions are very fast if compared to banking channels. A bitcoin transaction can be processed within 10 minutes. It doesn't matter if the transaction is local or international.

8.5 Government can't take it away

Government cannot take back your Bitcoins as it is decentralized and no one has control over it. The maximum is that the government can ban it but still your bitcoins has some value in those market/places/regions where it is still legal and thus can be cashed or used.

8.6 People can't steal payment information

Most online purchases today are made via credit cards, debit cards requiring to enter all your secret information (the credit card number, expiry date, and CVV number) into a web form. This is why credit card numbers keep being stolen.
Bitcoin transactions, however, don't require to give up any secret information.

9. DISADVANTAGES OF BITCOIN

9.1 Degree of acceptance

Bitcoins are still only accepted by a very small group of online merchants. This makes it unfeasible to completely rely on Bitcoins as a currency. Every day, more businesses accept bitcoins because they want the advantages of doing so, but the list remains small and still needs to grow in order to benefit from network effects.

9.2 Volatility

Bitcoins are subject to erratic changeability. Its value is not fixed as it keeps varying. Also, Bitcoins' value is not predictable. This rise and fall in the value also creates risk for investors who seek to earn profits. Speculators wish to take advantage of Bitcoin but genuine investors think of it as too risky and therefore all the investors do not invest in Bitcoin.

9.3 Ongoing development

Bitcoin software is still in beta with many incomplete features in active development. New tools, features, and services are being developed to make Bitcoin more secure and accessible to the masses. But still it might contain some technical flaws.

9.4 Possible government interference

Well the government may not take your bitcoins away but can ban it in the country, which will put an end to its use within the country.

9.5 Lack of recourse

If the wallet is corrupted, Bitcoins are essentially lost. There is nothing that can be done to recover it. However, these Bitcoins stay in the network. But there is no way to use these Bitcoins.

9.6 No buyer protection

Bitcoin transactions are irreversible. So when goods are bought using Bitcoins, and the seller doesn't send the promised goods, nothing can be done to reverse the transaction and the buyer has to face the loss.

9.7 Misuse in illegal activities

Bitcoins have become largely popular and demanding among individuals and organizations who practice illegal activities, such as trading weapons, drugs, money laundering and many other activities that are illegal and against the law. This is due to Bitcoin transactions providing anonymity to its users.

10. CONCLUSION

Bitcoin is a revolutionary payment system. Bitcoin is taking the world by storm, thanks to its innovative idea and unique features. It is currently the widely accepted cryptocurrency in the world. It is driven by the ease of transaction and the incentives to mine.

However, there is so much uncertainty around Bitcoin. For it to be widely used, its volatility needs to settle down quite a bit. It's currently a high risk currency that's totally unpredictable. Some people genuinely think this is the future. Others are terrified that it could destroy our economy. But many from both sides agree that if we could get Bitcoin to work or something like it, if we could trust a digital currency to work without the middleman, then the way the world economy functions, could be transformed for the better. Sure, Bitcoin has some disadvantages, but some of those are because Bitcoin is a new thing, so as time goes by, these problems will be resolved. Bitcoin might or might not be the major cryptocurrency of the future, but it is leading the way towards a more seamless digital global economy.

REFERENCES

- https://bitcoin.org/en/
- https://en.wikipedia.org/wiki/History_of_bitcoin
- https://www.coindesk.com/information/how-do-bitcoin-transactions-work/
- http://learnmeabitcoin.com/glossary/
- https://bitcoin.stackexchange.com/questions/12427/can-someone-explain-how-the-bitcoin-blockchain-works
- https://www.youtube.com/watch?v=kubGCSj5y3k