GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

BLOCKCHAIN TECHNOLOGY and CRYPTOCURRENCY IMPLEMENTATION

A Report for the Evaluation 3 of Project 2

Submitted by

ANKITA RASTOGI

(1613105015)

in partial fulfilment for the award of the degree

of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING WITH SPECIALIZATION OF CLOUD COMPUTING AND VIRTUALIZATION

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

Under the Supervision of
Dr. SATYAJEE SRIVASTAVA, M.Tech, Ph.D.,
Professor

APRIL / MAY- 2020

GALGOTIAS UNIVERSITY

SCHOOL OF COMPUTING AND SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Certified that this project report "BLOCKCHAIN TECHNOLOGY and CRYPTOCURRENCY IMPLEMENTATION" is the bonafide work of "ANKITA RASTOGI (1613105015)" who carried out the project works under my supervision

SIGNATURE OF HEAD
Dr. MUNISH SHABARWAL,
PhD (Management), PhD (CS)
PROFESSOR & DEAN,
School of Computing Science & Engineering

SIGNATURE OF SUPERVISOR
Dr. SATYJEE SRIVASTAVA, M.Tech, Ph.D.,
PROFESSOR & SUPERVISOR
School of Computing Science & Engineering

ACKNOWLEDGEMENT:

This is an excellent opportunity to acknowledge and to thanks, all those persons without whose support and help this project would be impossible. we might prefer to add some heartfelt words for those who were a part of this project in numerous ways.

I would prefer to because of my project guide Dr. SATYAJEE SRIVASTAVA, for his indefatigable guidance, valuable suggestion, moral support, constant encouragement, and contribution of your time for the successful completion of project work. I'm very grateful to him, for providing all the facilities needed during the project development. At the outset, I sincerely thank all faculty members of my institution GALGOTIAS UNIVERSITY for his extra effort to create our session online and inspire all ideas.

I would prefer to thank all those that helped me directly or indirectly. Last but not the smallest amount, I'd prefer to acknowledge the continuing support of my friends, whose patience and encouragement during these long days and nights are paramount in making this project a reality.

THANK YOU.

DECLARATION:

I hereby declare that this submission is my very own work which, to the simplest of my knowledge and belief, it contains no material previously published or written by another person nor material which to a considerable extent has been accepted for the award of the other degree or diploma of the university or other institute of upper learning, except where due acknowledgment has been made within the text.

I inform that every data used in this report if it's taken from any site is clearly referenced under the reference section.

SIGNATURE

Ankita Rastogi

16SCSE105107

Date: 13-may-2020

ABSTRACT:

Data's are getting created these days and the number of users of the internet system growing rapidly leads to the formation of multiple useful information, which can be very confidential and might have value more than a jewel. These important data are created by millions of people working over the internet. This protection of the user data is leading the way for more and more public to use internet and save their data online. The internet security started with cryptography and now as you have heard there are various other algorithms and techniques are formed to protect our data. Among all these the term Blockchain is much in demand and people tend to use it and also some suggest it as the future of the internet system. Blockchain is nothing but keeping record of our ledger by binding them in blocks with chain virtually. In this paper, I will be discussing about the basic Blockchain and its formation along with its advantages and disadvantages. Later, I will discuss about some of the use-cases and importance of blockchain; say in Agriculture, Healthcare and Education. These are the three main areas of discussion about blockchain evolution. A practical implementation of the blockchain has been explained briefly using the basic concepts of bitcoin. Putting aside all the hype around the price of Bitcoin and other cryptocurrencies, the goal of this blog post is to give you a practical introduction to blockchain technology. Covering some core concepts behind blockchain, while explaining how to implement a blockchain using Python. We will also implement web applications to make it easy for end users to interact with our blockchain. Please note that we are using Bitcoin here as a medium for explaining the more general technology of "Blockchain", and most of the concepts described are applicable to other blockchain use cases and crypto-currencies.

TABLE OF CONTENTS:

LIST OF TABLES:

LISTS OF FIGURES:

LISTS OF ABBREVIATION:

TITLE	ABBREVIATION
1. P2P	Peer to Peer
2. UN	United Nation
3. US	United States
4. CO-OP	Cooperative
5. RSA	Rivest, Shamir, Adleman
6. API	Application user interface
7. URL	Uniform resource locator
8. BTC	Bitcoin
9. RBI	Reserve Bank of India
10. SC	Supreme Courts
11. TCP/IP	Transmission control protocol
12. POW	Power of Work
13. MB	Megabyte
14. NGO	Non-Governmental Organization

CHAPTER 1
INTRODUCTION

Blockchain technology is the growing invention which includes a chain of blocks. A **Blockchain** is a distributed or a **digital ledger**, which is primarily created to record the details of each financial and non-financial transaction. The absolute and permanent data is stored in a distributed database. The entire record is completely transparent which means that anyone who is linking to the network is able to view the transactions. Fundamentally, the **Blockchain technology** is the combination of three technologies, i.e. private key cryptography, P2P network, and the program. The **Blockchain technology** has shown its revolution in the field of information registration and distribution which removes the requirement for an intermediary expert to enable the digital relationships.

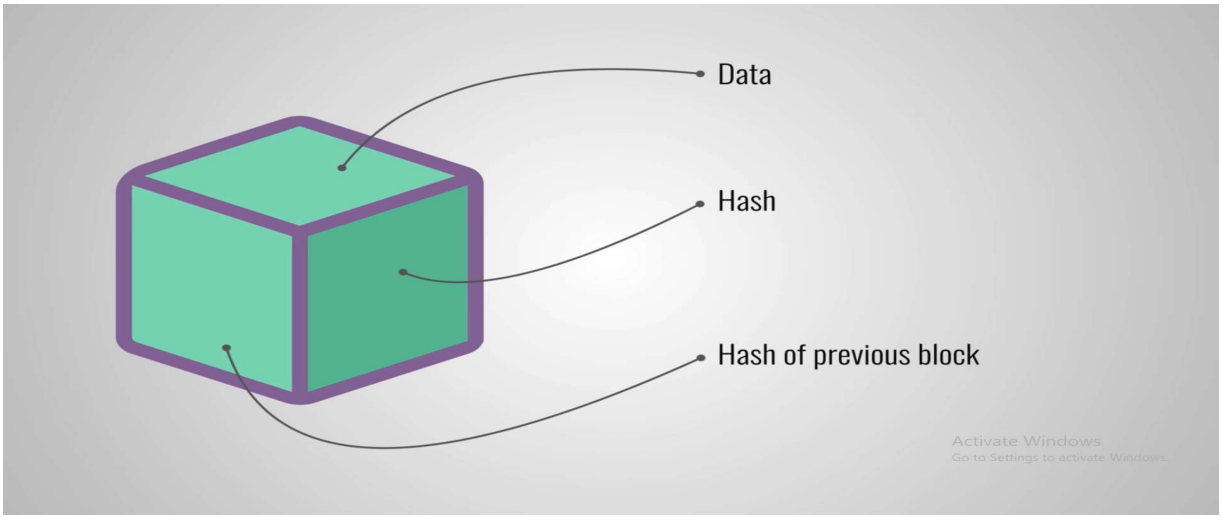

Fig 1: basics of blockchain

Blockchain technology has provided the most popular product, i.e. Bitcoin which is a type of cryptocurrency and functions as a public ledger for all transactions happening on the network. It has resolved the problem of double spending, unauthorized spending, and thus increasing security. It also helps to remove the need for an intermediary expert. Since there has been a substantial increase in the number of cyber-attacks recently, the **Blockchain technology** help to attract the varied audience.

1.1 THE OVERALL DESCRIPTION:

By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.

Blockchain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. The identity of Satoshi Nakamoto is unknown. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications, and blockchains that are readable by the public are widely used by cryptocurrencies. Blockchain is considered a type of payment rail. Private blockchains have been proposed for business use.

According to the UN Food and Agriculture Organization, 2.5 billion people in developing economics derived their livelihood from agriculture in 2011; that was over a third of the world's population.

1 Yet, without farming sophistication, business knowledge, financial resources, and leverage against much larger buyers—not to mention corrupt intermediaries and government officials—developing world farmers receive only a tiny share of the ultimate value of their crops. For instance, Kenyan farmers reported receiving only 30 cents per kilogram for their coffee, which retailed for more than 100 times that price.

2 Blockchain is a revolutionary technology that implements a shared ledger or database to deliver an immutable, single version of the truth among numerous,

sometimes adversarial, stakeholders. Blockchain provides transparency to inefficient and corrupt business practices by enabling equitable participation for farmers and other stakeholders on the global food value chain, leading to greater prosperity for developing world agricultural workers. Where in agriculture can we best fulfil this promise? First, it is in provenance and traceability for food safety. Every year, one in ten people fall ill—and 400,000 die—because of contaminated food.

3 Food safety failures are magnified, last longer, and cost more because of lack of access to information and traceability. In the summer of 2017, the US Food and Drug Administration took two months to trace salmonella-tainted papayas consumed in the States back to a Mexican farm where the contamination originated. Using blockchain, global supply chain participants can gain permissioned access to trusted information regarding food provenance. They could then access data on the blockchain network to trace contaminated products expeditiously, stemming public health outbreaks, and potentially saving lives.

4.A second class of blockchain applications is the support of farmer cooperatives at the local level, especially in developing worlds. Cooperatives pool individual farmers' resources, giving the collective more leverage over large buyers and inefficient or corrupt middlemen. As legal stakeholders, co-op members are inherently interested in sustainable agriculture practices that "minimize tilling and

water use, encourage healthy soil by planting fields with different crops year after year and integrating croplands with livestock grazing, and avoid pesticide use by nurturing the presence of organisms that control crop-destroying pests."

5 Blockchain can help co-op farmers retain more of their profits, ensuring that they will not have to forsake long-term sustainability practices in exchange for the short-term need to turn a profit. Sustainable agriculture is complementary to local, community-based economics, wherein the goal is to have producers and buyers transact locally and, therefore, retain economic value in the community.

The major purposes of agricultural environmental monitoring systems include supporting early warning systems, and measuring baseline data that policy makers and resources managers can use in planning. Yet, bias is an 'inherent human-related challenge' that propagates to group bias among groups of like-minded individuals. For example, stakeholders' biases and preferences correlate highly with the mission of their represented organizations. In a study about environmental and energy applications of Multi-Criteria Decision Analysis, Maternofetal showed that the most important factor affecting objective prioritization biases are the people involved in the decision-making process. NGOs can also demonstrate bias by putting disproportionate focus on an issue relative to other comparable issues. Dixon and Richards explain why governments bias capital-intensive large agriculture systems to maximize inexpensive food supplies from rural agriculture to urban infrastructure,

where the majority of elected officials' constituents reside. By distributing database management among a greater number of actors, and making system wide data manipulation more difficult, baseline agricultural environmental data integrity is maintained–safeguarded from the biases or the fraudulent activity of any individual group of farmers, NGOs, stakeholders, consumers, and decision makers.

One of the best features of Blockchain that could benefit the Healthcare sector is its quality of decentralization, because of this reason a lot of data is kept in small units. If this data centralizes, the content of data would have been stored in a particular system and anyone can have access to the system who could have corrupted all the data.

The healthcare business is drowning in data—clinical trials, patient medical records, complicated asking, medical analysis and additional. Adoption Associate in the nursing implementation of blockchains is going to be an evolution over time as blockchains applications square measure vetted and adopted in addition because of the business returning along to work out collaboration and governance problems. Because it is continuously with new technology, the total prospects of what could transpire in the future are now unknown.

- A blockchain is essentially a digitally-signed financial ledger. Each transaction on the blockchain is visible on the public ledger, and all entries are distributed across the network, requiring consensus about each transaction.

- Each transaction executed in the system becomes part of the blockchain, but only after a certain number of nodes reaches a consensus that the transaction is valid. Then, the transaction is added to the blockchain in a new block.
- Consensus means if you modify any of the block from the network, that block is modified at every user end in the same network.

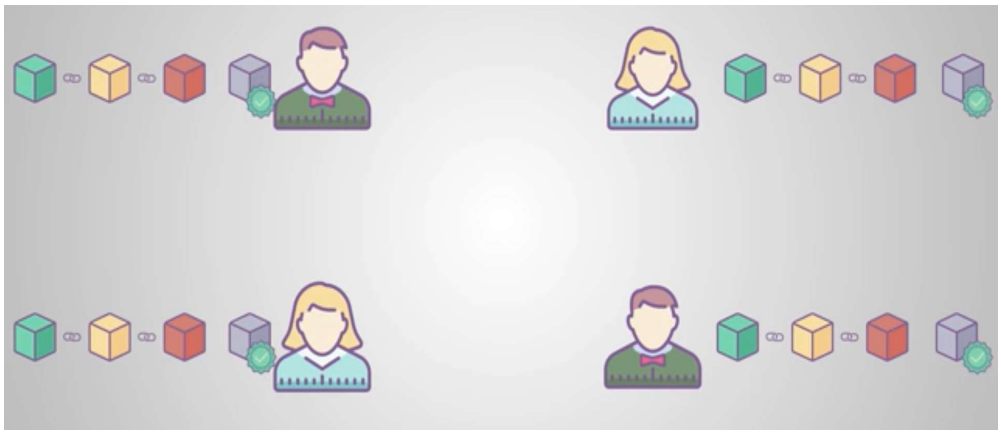

Fig 2: consensus

- it is the technology which aims at maintaining a ledger with a cryptographic signature.
- Blockchain is nothing but the connection of all our data with each other by the help of a virtual chain.
- Whenever a new addition in the market with the same signature is detected it gets attached to the chain of its similar signature. This is how small blocks of valuable information is created and they all are linked to each other with the help of virtual chains and altogether they are called blockchain

1.2 PURPOSE:

Blocks" on the blockchain are made up of digital pieces of information. Specifically, they have three parts:

1. Blocks store information about transactions like the date, time, and dollar amount of your most recent purchase from Amazon. (NOTE: This Amazon example is for illustrative purchases; Amazon retail does not work on a blockchain principle as of this writing)
2. Blocks store information about who is participating in transactions. A block for your splurge purchase from Amazon would record your name along with Amazon.com, Inc. (AMZN). Instead of using your actual name, your purchase is recorded without any identifying information using a unique "digital signature," sort of like a username.
3. Blocks store information that distinguishes them from other blocks. Much like you and I have names to distinguish us from one another, each block stores a unique code called a "hash" that allows us to tell it apart from every other block. Hashes are cryptographic codes created by special algorithms. Let's say you made your splurge purchase on Amazon, but while it's in transit, you decide you just can't resist and need a second one. Even though the details of

your new transaction would look nearly identical to your earlier purchase, we can still tell the blocks apart because of their unique codes.

While the block in the example above is being used to store a single purchase from Amazon, the reality is a little different. A single block on the Bitcoin blockchain can actually store up to 1 MB of data. Depending on the size of the transactions, that means a single block can house a few thousand transactions under one roof.

1.3 MOTIVATION AND SCOPE:

Blockchain technology accounts for the issues of security and trust in several ways. First, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. If you take a look at Bitcoin's blockchain, you'll see that each block has a position on the chain, called a "height." As of January 2020, the block's height had topped 615,400.

After a block has been added to the end of the blockchain, it is very difficult to go back and alter the contents of the block. That's because each block contains its own hash, along with the hash of the block before it. Hash codes are created by a math function that turns digital information into a string of numbers and letters. If that information is edited in any way, the hash code changes as well.

Here's why that's important to security. Let's say a hacker attempts to edit your transaction from Amazon so that you actually have to pay for your purchase twice. As soon as they edit the dollar amount of your transaction, the block's hash will change. The next block in the chain will still contain the old hash, and the hacker would need to update that block in order to cover their tracks. However, doing so would change that block's hash. And the next, and so on.

In order to change a single block, then, a hacker would need to change every single block after it on the blockchain. Recalculating all those hashes would take an enormous and improbable amount of computing power. In other words, once a block is added to the blockchain it becomes very difficult to edit and impossible to delete.

To address the issue of trust, blockchain networks have implemented tests for computers that want to join and add blocks to the chain. The tests, called "consensus models," require users to "prove" themselves before they can participate in a blockchain network. One of the most common examples employed by Bitcoin is called "proof of work." In the proof of work system, computers must "prove" that they have done "work" by solving a complex computational math problem. If a computer solves one of these problems, they become eligible to add a block to the blockchain. But the process of adding blocks to the blockchain, what the cryptocurrency world calls "mining," is not easy. In fact, the odds of solving one of

these problems on the Bitcoin network were about one in 15.5 trillion in January 2020.[1] to solve complex math problems at those odds, computers must run programs that cost them significant amounts of power and energy (read: money). Proof of work does not make attacks by hackers impossible, but it does make them somewhat useless. If a hacker wanted to coordinate an attack on the blockchain, they would need to control more than 50% of all computing power on the blockchain so as to be able to overwhelm all other participants in the network. Given the tremendous size of the Bitcoin blockchain, a so-called 51% attack is almost certainly not worth the effort and more than likely impossible.

1.4 TYPES AND CHARACTERISTICS:

	Public	Consortium	Private
Participants	Without permission • Anonymous • Could be malicious	Permissioned • Identified • Trusted	Permissioned • Identified •Trusted
Consensus mechanisms	Proof of work, proof of stake, etc. • Large energy consumption • No finality • 51% attack	Voting or multi-party consensus algorithm • Lighter • Faster • Low energy consumption • Enable finality	Voting or multi-party consensus algorithm • Lighter • Faster • Low energy consumption • Enable finality
Transaction approval freq.	Long Bitcoin: 10 min or more	Short 100× ms	Short 100× ms

table 1: types of blockchain

CHAPTER 2
LITERATURE SURVEY

2.1 LITERATURE REVIEW:

Blockchain is the technology which has been first suggested in 1991 and further developed in 2008 and 2016. People see blockchain as an opportunity to make the market fair for every individual. Some say it is one of the very best way to decentralize the system of market where all the rights are distributed among its each member. The only Question, what is blockchain can be answered, as it is the technology which aims at maintaining a ledger with a cryptographic signature. Whenever a new addition in the market with the same signature is detected it gets attached to the chain of its similar signature. This is how small blocks of valuable information is created and they all are linked to each other with the help of virtual chains and altogether they are called blockchain. Blockchain is nothing but the connection of all our data with each other by the help of a virtual chain. Again, the confusion arises when it is said that it is process of decentralization. Decentralization is the process in which the main is taken down and the power is divided among all the members equally. For example, if decentralization occurs in the country then the government will be taken down and the right of decision will be divided among the general public. Even the revolutionary giants such as Facebook, Google, Instagram etc sows the public only limited data which they want us to be looked into but much

of it hidden as a protection act, while in decentralization there will be nothing hidden and all will be under the control of pubic. Decentralization process uses TCP/IP protocol to manage the connection from peer-to-peer (P2P). Total stabilize connection establishment is important as every member of the group will be participating taking the decision. If in case any of the block fails to connect there are chances of non-redemption. It can highly impact the finance system of the country as it has huge impact on the economy. After people knew about the concept of blockchain and the uses of it has demand all over the world. Its market has risen to 60,000 from the day it has started. There is no doubt that will keep the data secure and robust so it is very trustworthy. Imagine some ledger you are maintaining which can't be stolen by anyone and nobody can interfere or make changes in the same. Bitcoin is one of the applications of blockchain. Not to be confused between bitcoin and blockchain because people didn't know sometimes and get confused between these two, bitcoin is the application of blockchain which is used for money transfer across the world without the 3rd party interference (e.g. bank). This makes sure that none of the money is spent between the transfer and gives a secured and trusted platform. Current bitcoin price for ₹515371.64= 1Bitcoin. Earlier it was not legal to use the cryptocurrency as means of transferring money but as per the orders from SC now Indian market is expected to grow in the cryptocurrency transactions. RBI strictly opposes the decision but that is a later discussion. Let us now understand the

functioning of blockchain. The blockchain starts works as when in the network a transaction is initiated. Firstly, the transaction is recorded and then it is made into a box like structure which contains all the encrypted data and the values. The block is shared between all the nodes (meaning all the members of the chain). The nodes then verify if the transaction is valid or not and it okay to be inserted in the chain. The nodes which verifies this is awarded with some benefits and later on the block gets added in the blockchain. The transaction completes and it adds the new block in chain. The node verifying the authenticity of the block is called mining. Mining uses various algorithm and techniques to verify the block and makes sure that the forgery is not being made and decentralization of the data. Blockchain has been in demand for a very long time now and its application are expected to grow and be robust by time. It has many advantages and disadvantages as of now but in near future it is expected to be very secured. Blockchain has shown its advantage in finance sector a lot. Maintaining an online contract to e-governance system the life has grown easier. According to Deloitte's blockchain survey of 2018-2019 gives the following data about views of blockchain relevance within organizations. According to the same survey conducted by Deloitte the country wise view and adaptation of blockchain has found to be different. The comparison report of china, Israel, Singapore and united states is studied and it has been found that people agreeing on different questions are as follows: Blockchain will disrupt the industry: China-34%,

Singapore-27%, Isreal-15%, US-22%, Already bought blockchain in production China-16%, Singapore-19%, Isreal-2%, US-29%, Blockchain as top five strategic priority China-73%, Singapore-50%, Isreal-40%, US-56%.

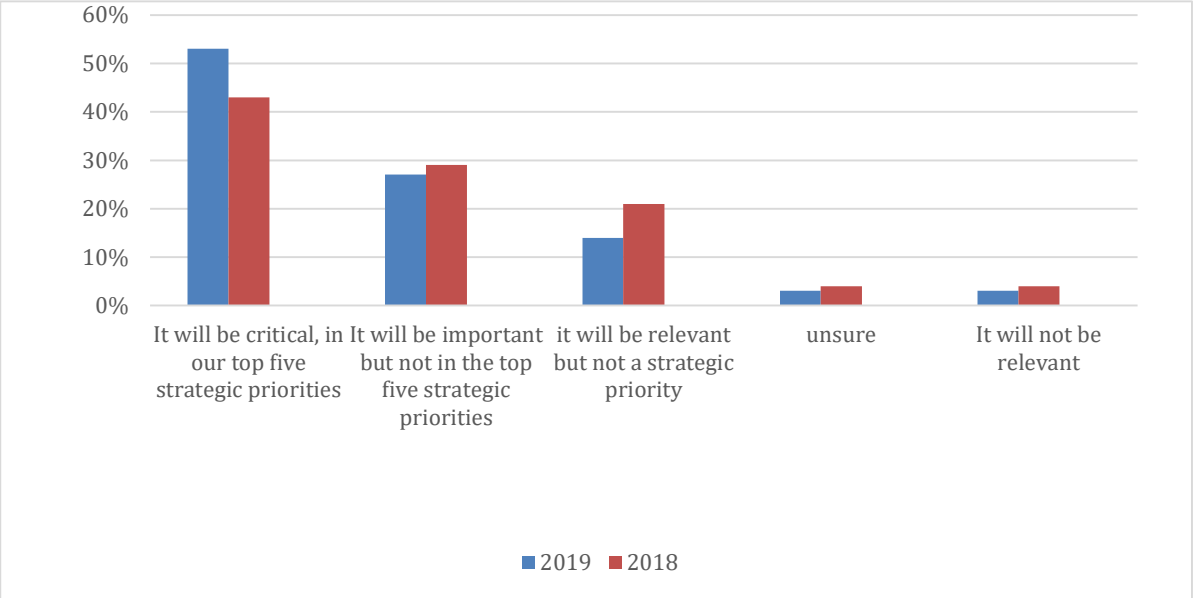

Fig 3: Swot analysis

The above data is sufficient to say that all over the world the acceptance of blockchain technology has increased and people are taking steps to adapt this technology to improve their organisation and stay the most updated. Soon there will be the change of era and adaptability of blockchain in market will lead us to the very new way of thinking and development. There will be decentralized organization where there will be no boss to measure your work but you yourself will be measuring your day's work and improving yourself. This is all about making everything secured and reliable for everyone. Where dependency will be less and we can expect higher results.

2.2 PRINCLIPLE OF BLOCKCHAIN:

Blockchain works on three principle:

1. TRANSPARENCY
2. DECENTRALIZATION
3. IMMUTABILITY
4. DOUBLE SPENDING
5. PEER TO PEER TRANSFER
6. CONSENSUS

2.3 HOW DOES BLOCKCHAIN WORK?

The blockchain is like a decentralized bank ledger, in both cases the ledger is a record of transactions and balances. When a cryptocurrency transaction is made, that transaction is sent out to all users hosting a copy of the blockchain. Specific types of users called miners then try to solve a cryptographic puzzle (using software) which lets them add a “block” of transactions to the ledger. Whoever solves the puzzle first gets a few “newly mined” coins as a reward (they also get transaction fees paid by those who created the transactions). Sometimes miners pool computing power and share the new coins. The algorithm relies on consensus. If the majority of users trying to solve the puzzle all submit the same transaction data, then it confirms that the transactions are correct. Further, the security of the blockchain relies cryptography. Each block is connected to the data in the last block via one-way

cryptographic codes called hashes which are designed to make tampering with the blockchain very difficult. Offering new coins as rewards, the difficulty of cracking the cryptographic puzzles, and the amount of effort it would take to add incorrect data to the blockchain by faking consensus or tampering with the blockchain, helps to ensure against bad actors.

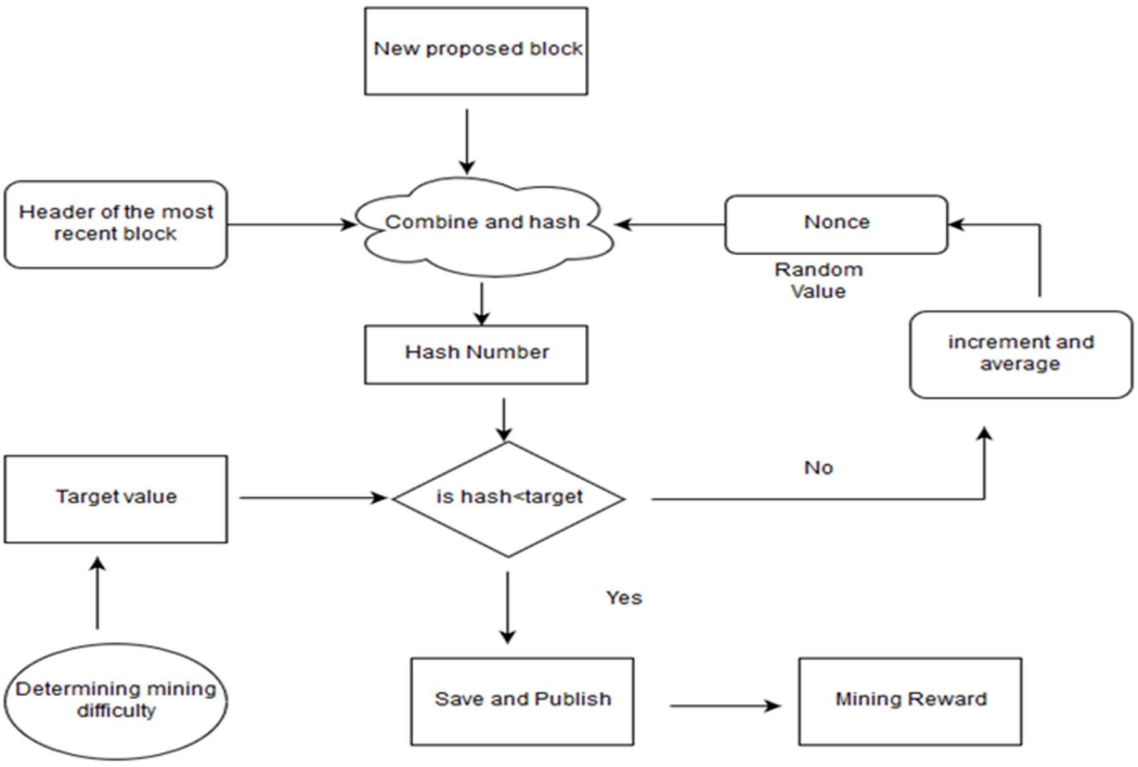

Fig 4: working of blockchain

Blockchain is a distributed ledger system, or it is just like a record book but it not maintained by one person, it is decentralized, and any interested person can keep and maintain the record book. The blockchain is a new and revolutionary concept in technology that's why more techies are interested

in it. But it has its *Advantages and Disadvantages*, so look at them one by one.

2.4 ADVANTAGES:

1. It is a Decentralized System.
2. The blockchain is transparent.
3. The blockchain is more secure
4. Faster and cost effective.
5. It is immutable.
6. No downtime
7. It can save historical and current data at same place.
8. User empowers.

2.5 DISADVANTAGES:

1. Complexity.
2. Size of blockchain
3. Human errors
4. Need more resources
5. Power consumption and security issues
6. Speed and scalability.

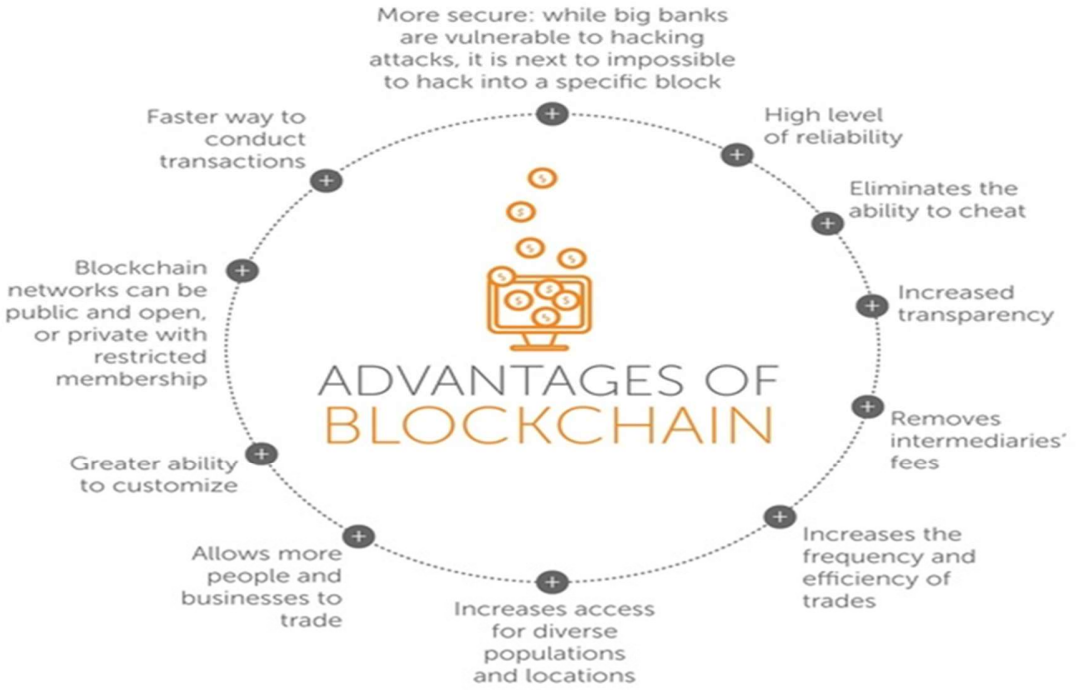

Fig 5: advantages of blockchain

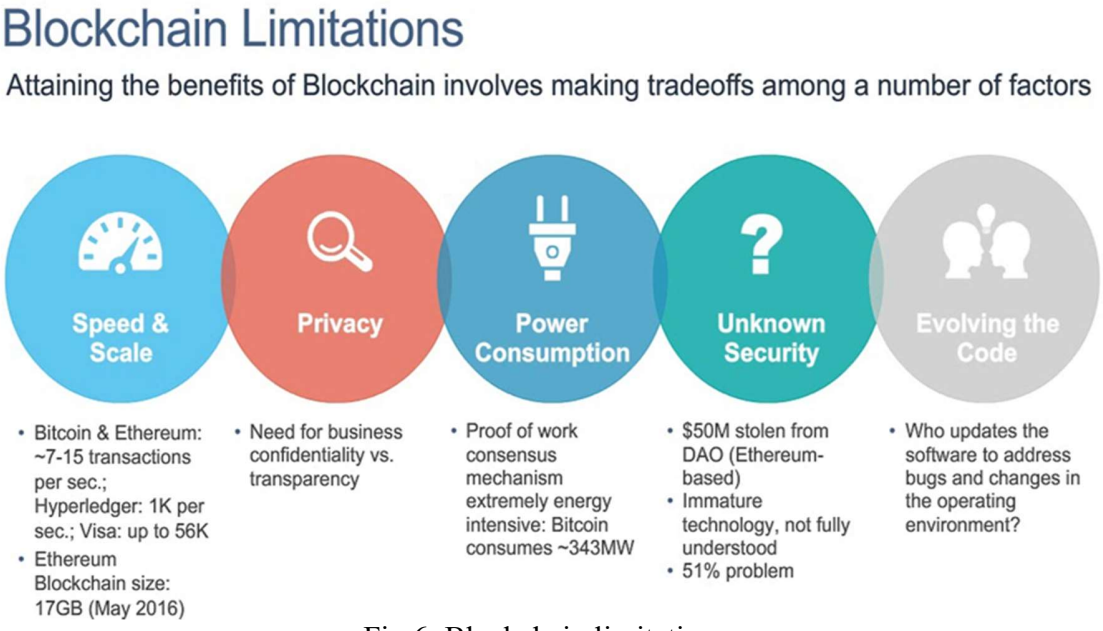

Fig 6: Blockchain limitation

Chapter-3
CRYPTOCURRENCY INTRODUCTION

3.1 CRYPTO+CURRENCY:

Cryptocurrency is roughly the equivalent of using PayPal or a Debit Card**,** except the numbers on the screen represent cryptocurrency instead of dollars. All a new user needs to do is set up a Coinbase account or download the Cash App to get started**.** With Coinbase users can buy, sell, send, receive, and store Bitcoin, Bitcoin Cash, Ether, and Litecoin (Coinbase provides an all-in-one wallet, broker, and exchange service making them a one-stop-shop for new users). With Cash App users can buy, sell, send, receive, and store Bitcoin.

The basic concepts are:

To use cryptocurrency, you don't need to understand it (any more than you need to understand the monetary system to use a debit card). However, if you want to understand cryptocurrency you need to understand the concept of digital currency**,** the concept of blockchain (both as a public ledger of transactions and a technology), and the concept of cryptography. After-all, cryptocurrency is a digital currency, where transactions are recorded on a public digital ledger called a blockchain, and every process along the way is secured by cryptography. The goal of this page will be to help you understand these things and how they connect.

Cryptocurrency works a lot like bank credit on a debit card. In both cases, a complex system that issues currency and records transactions and balances works behind the scenes to allow people to send and receive currency electronically. Likewise, just like with banking, online platforms can be used to manage accounts and move balances. The main difference between cryptocurrency and bank credit is that instead of banks and governments issuing the currency and keeping ledgers, an algorithm does.

3.2 What is cryptocurrency?

Cryptocurrency is best thought of as digital currency (it only exists on computers). It is transferred between peers (there is no middleman like a bank). Transactions are recorded on a digital public ledger (called a "blockchain"). Transaction data and the ledger are encrypted using cryptography (which is why it is called "crypto" "currency"). It is decentralized, meaning it is controlled by users and computer algorithms and not a central government. It is distributed, meaning the blockchain is hosted on many computers across the globe. Meanwhile, cryptocurrencies are traded on online cryptocurrency exchanges, like stock exchanges. Bitcoin (commonly traded under the symbol BTC) is one of many cryptocurrencies; other cryptocurrencies have names like "Ether (ETH)," "Ripple (XRP)," and "Litecoin (LTC)." Alternatives to Bitcoin are called "altcoins."

3.3 How does cryptocurrency work?

Transactions are sent between peers using software called “cryptocurrency wallets.” The person creating the transaction uses the wallet software to transfer balances from one account (AKA a public address) to another. To transfer funds, knowledge of a password (AKA a private key) associated with the account is needed. Transactions made between peers are encrypted and then broadcast to the cryptocurrency’s network and queued up to be added to the public ledger. Transactions are then recorded on the public ledger via a process called “mining” (explained below). All users of a given cryptocurrency have access to the ledger if they choose to access it, for example by downloading and running a copy of the software called a “full node” wallet (as opposed to holding their coins in a third-party wallet like Coinbase). The transaction amounts are public, but who sent the transaction is encrypted (transactions are pseudo-anonymous). Each transaction leads back to a unique set of keys. Whoever owns a set of keys, owns the amount of cryptocurrency associated with those keys (just like whoever owns a bank account owns the money in it). Many transactions are added to a ledger at once. These “blocks” of transactions are added sequentially by miners. That is why the ledger and the technology behind it are called “block” “chain.” It is a “chain” of “blocks” of transactions.

TIP: I’ve just described how Bitcoin works and how many other coins work too. However, some altcoins use unique mechanics. For example, some coins offer fully private transactions and some don’t use blockchain at all.

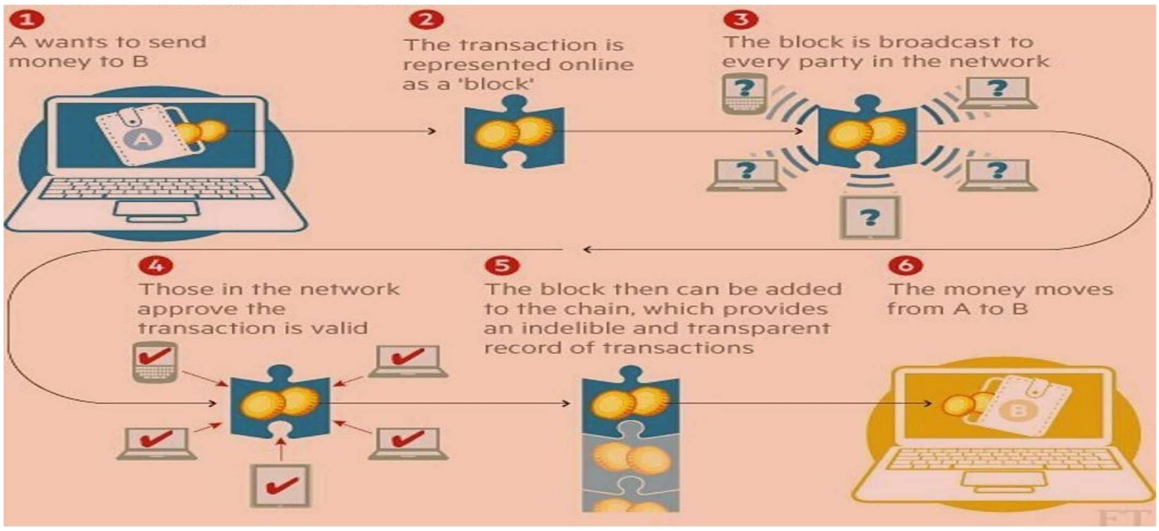

Fig 7: flowchart of cryptocurrency

3.4 What is cryptocurrency mining? People who are running software and hardware aimed at confirming transactions to the digital ledger are cryptocurrency miners. Solving cryptographic puzzles (via software) to add transactions to the ledger (the blockchain) in the hope of getting coins as a reward is cryptocurrency mining.

3.5 How does cryptography work with cryptocurrency? The keys that move balances around the blockchain utilize a type of one-way cryptography called public-key cryptography. The “hashes” (the one-way cryptographic codes that tie together blocks on the blockchain) use a similar type of cryptography. Meanwhile, transaction data sent and stored on the blockchain is tokenized (tokenization is a type of one-way cryptography that points to data but doesn’t contain all the original data). The key to understanding these layers of encryption

which ensure a system like Bitcoin's (some coins work a little differently) is found in one-way cryptographic functions (cryptographic hash functions, cryptographic tokens, and public-key cryptography are all names for specific, but related, types of one-way cryptographic functions). The main idea is that cryptocurrency uses a type of cryptography that is easy to compute one way, but hard to compute the other way without a "key." Very loosely you can think of it like this, it is easy to create a strong password if you are in your online bank account, but very hard for others to guess a strong password after it has been created.

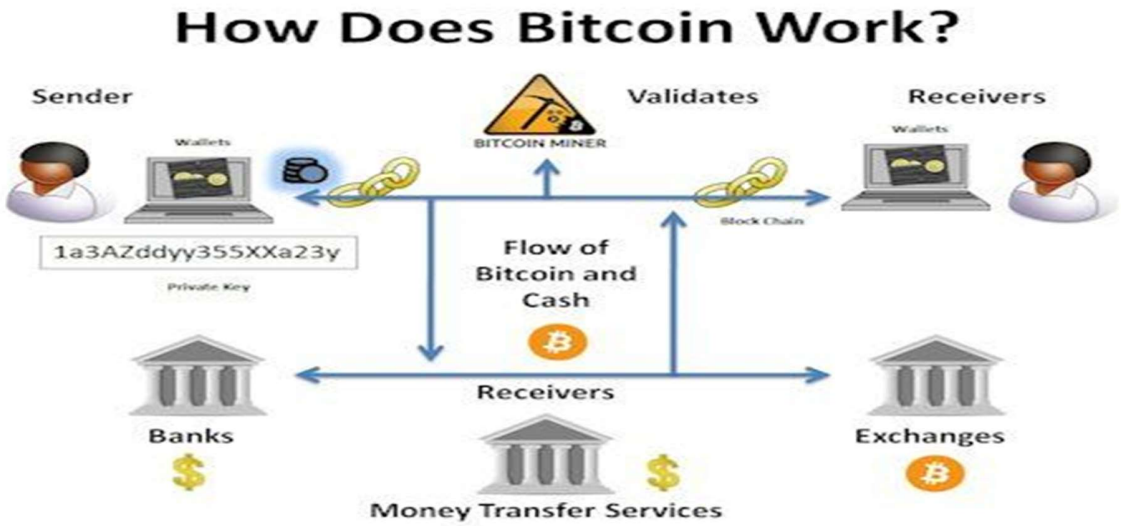

Fig 8: how does bitcoin work?

3.6 How does one obtain or trade cryptocurrency? Cryptocurrency can be obtained most of the same ways other types of currencies can. You can exchange goods and services for cryptocurrency, you can trade dollars for cryptocurrencies, or you can trade cryptocurrencies for other cryptocurrencies. Trading is generally done via brokers and exchanges. Brokers are third parties that buy/sell cryptocurrency,

exchanges are like online stock exchanges for cryptocurrency. One can also trade cryptocurrencies directly between peers. Peer-to-peer exchanges can be mediated by a third party, or not. Please be aware that cryptocurrency prices tend to be volatile. One should ease into cryptocurrency investing and trading and be ready to lose everything they put in (especially if they invest in or trade alternative coins with lower market caps).

CHAPTER 4
PROPOSED MODEL

A cryptocurrency is a digital medium of exchange that relies on cryptography to secure and verify transactions. Most cryptocurrencies, such as bitcoin, are decentralized and consensus-based. the basic requirements for our new payment system:

1. All transactions should be made over the Internet
2. We do not want to have a central authority that will process transactions
3. Users should be anonymous and identified only by their virtual identity
4. A single user can have as many virtual identities as he or she likes
5. Value supply (new virtual bills) must be added in a controlled way

Suppose that Alice wants to pay Bob 1$. If Alice and Bob use physical cash, then Alice will no longer have the 1$ after the transaction is executed. If Alice and Bob use digital money, then the problem gets more complicated. Digital money is in digital form and can be easily duplicated. If Alice sends a digital file worth 1$ to Bob by email for example, Bob cannot know for sure if Alice has deleted her copy of the file. If Alice still has the 1$ digital file, then she can choose to send the same file to Carol. This problem is called double-spending. One way of solving the double-spending problem is to have a trusted third party (a bank for example) between Alice, Bob and all other participants in the network. This third party is

responsible for managing a centralized ledger that keeps track of and validates all the transactions in the network. The drawback of this solution is that for the system to function, it requires trust in a centralized third party.

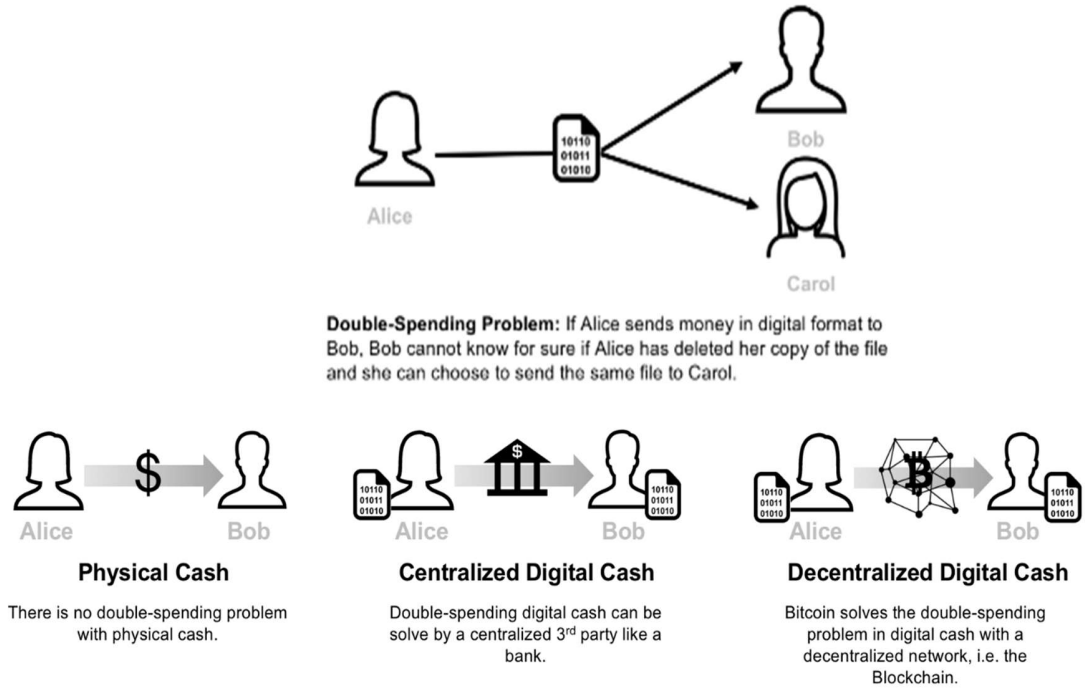

Fig 9: Double spending problem solution

- Cryptocurrency is a way to transfer anonymous value/information from one user to another in a distributed peer-to-peer network.
- Transactions are sent between peers using software called cryptocurrency wallets.
- The person creating the transaction uses the wallet software to transfer balances from one account (AKA a public address) to another. To transfer

funds, knowledge of a password (AKA a private key) associated with the account is needed.

- Transactions made between peers are encrypted and then broadcast to the cryptocurrency network and queued up to be added to the public ledger.
- Transactions are then recorded on the public ledger via a process called mining.

- The transaction amounts are public, but who sent the transaction is encrypted (transactions are pseudo-anonymous).
- Each transaction leads back to a unique set of keys. Whoever owns a set of keys, owns the amount of cryptocurrency associated with those keys (just like whoever owns a bank account owns the money in it).
- Many transactions are added to a ledger at once. These "blocks" of transactions are added sequentially by miners. That is why the ledger and the technology behind it are called "block" "chain."
- It is a "chain" of "blocks" of transactions. However, some altcoins use unique mechanics. For example, some coins offer fully private transactions and some don't use blockchain at all.

To solve the double-spending problem, Satoshi proposed a public ledger, i.e., Bitcoin's blockchain to keep track of all transactions in the network. Bitcoin's blockchain has the following characteristics:

- **Distributed**: The ledger is replicated across a number of computers, rather than being stored on a central server. Any computer with an internet connection can download a full copy of the blockchain.
- **Cryptographic**: Cryptography is used to make sure that the sender owns the bitcoin that she's trying to send, and to decide how the transactions are added to the blockchain.
- **Immutable**: The blockchain can be changed in append only fashion. In other words, transactions can only be added to the blockchain but cannot be deleted or modified.
- **Uses Proof of Work (PoW):** A special type of participants in the network called miners compete on searching for the solution to a cryptographic puzzle that will allow them to add a block of transactions to Bitcoin's blockchain. This process is called Proof of Work and it allows the system to be secure (more on this later).

CHAPTER 5
METHODOLOGY USED

There should be previous knowledge of some security algorithms and attacks before studying this system:

5.1 RSA

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e**. Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and Private key is kept private. The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So, if somebody can factorize the large number, the private key is compromised. Therefore, encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024-bit keys could be broken in the near future. But till now it seems to be an infeasible task. You need to create a **private key** and a **public key**. These two keys will be in some kind of mathematical correlation and will depend on each other. The algorithm that you will use to make these keys will assure that each private key will have a different

public key. As their names suggest, a private key is information that you will keep just for yourself, while a public key is information that you will share.

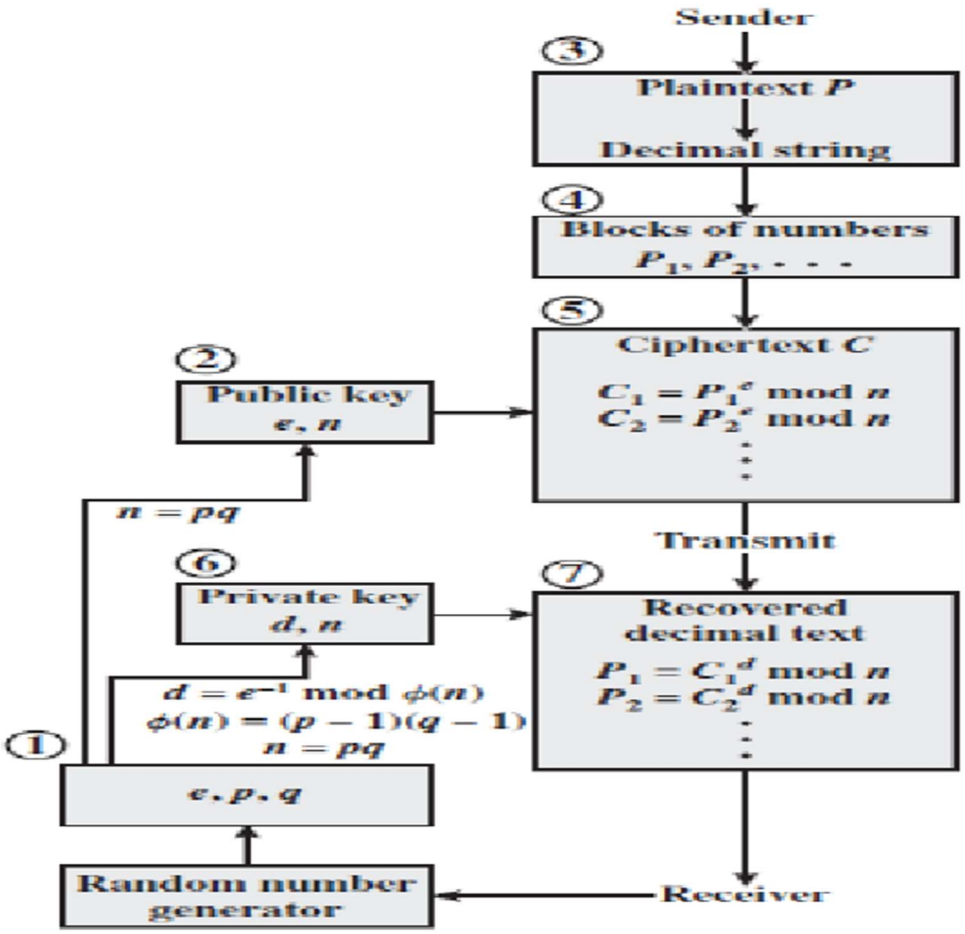

Fig 10: Flowchart of RSA

5.2 Digital Signature:

When signing a paper, all you need to do is append your signature to the text of a document. A digital signature is similar: you just need to append your personal data to the document you are signing. If you understand that the hashing algorithm adheres to the rule where **even the smallest change in input data must produce significant difference in output,** then it is obvious that the HASH value created for

the original document will be different from the HASH value created for the document with the appended signature. A combination of the original document and the HASH value produced for the document with your personal data appended is a **digitally signed document**. And this is how we get to your **virtual identity**, which is defined as the data you appended to the document before you created that HASH value. Next, you need to make sure that your signature cannot be copied, and no one can execute any transaction on your behalf. The best way to make sure that your signature is secured, is to keep it yourself, and provide a different method for someone else to validate the signed document. Again, we can fall back on technology and algorithms that are readily available. What we need to use is **public-key cryptography** also known as **asymmetric cryptography**. To make this work, you need to create a **private key** and a **public key**. These two keys will be in some kind of mathematical correlation and will depend on each other. The algorithm that you will use to make these keys will assure that each private key will have a different public key. As their names suggest, a private key is information that you will keep just for yourself, while a public key is information that you will share. If you use your private key (your identity) and original document as input values for the **signing algorithm** to create a HASH value, assuming you kept your key secret, you can be sure that no one else can produce the same HASH value for that document. If anyone needs to validate your signature, he or she will use the original

document, the HASH value you produced, and your public key as inputs for the **signature verifying algorithm** to verify that these values match.

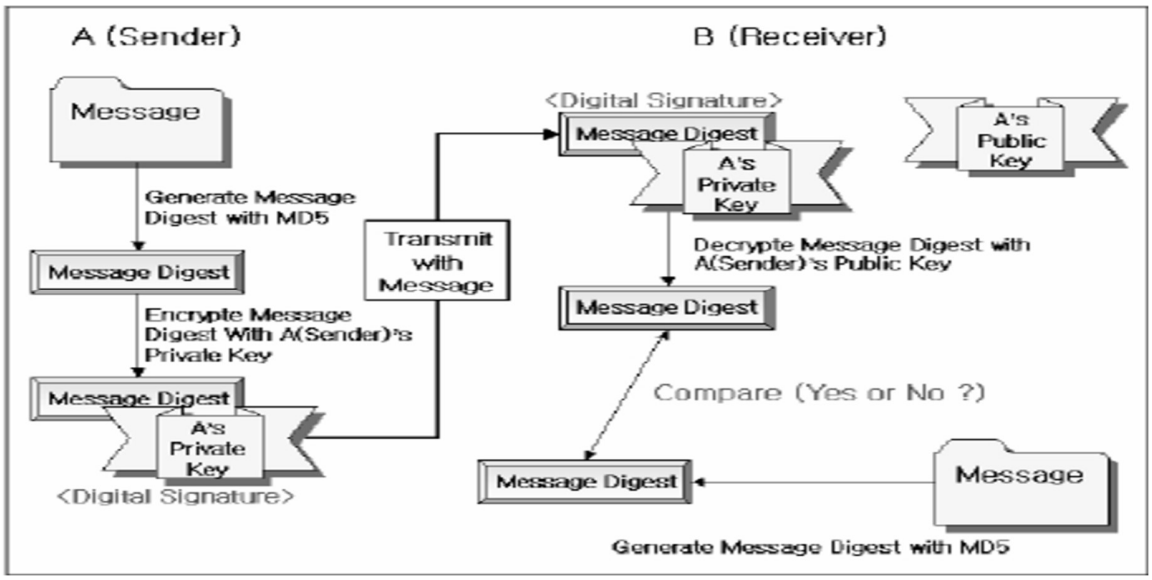

Fig 11: flowchart of digital signature

5.3 Hashing algorithm:

hashing is a process of taking some information that is readable and making something that makes no sense at all. each new block uses the previous block's hash as part of its data. To create a new block, a miner selects a set of transactions, adds the previous block's hash and mines the block in a similar fashion described above. Any changes to the data in any block will affect all the hash values of the blocks that come after it and they will become invalid. This give the blockchain its immutability characteristic. There are a few requirements that a good hashing algorithm needs:

1. Output length of hashing algorithm must be fixed (a good value is 256 bytes)

2. Even the smallest change in input data must produce significant difference in output
3. Same input will always produce same output
4. There must be no way to reverse the output value to calculate the input
5. Calculating the HASH value should not be compute intensive and should be fast

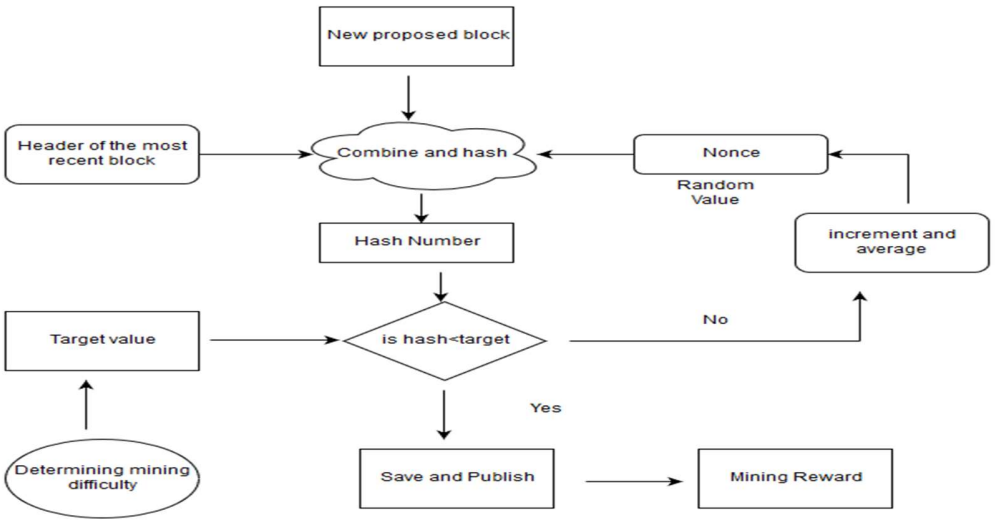

Fig 12: flowchart of hashing algorithm

5.4 Adding blocks to chain

If 2 miners solve a block at almost the same time, then we will have 2 different blockchains in the network, and we need to wait for the next block to resolve the conflict. Some miners will decide to mine on top of blockchain 1 and others on top of blockchain 2. The first miner to find a new block resolves the conflict. If the new block was mined on top of blockchain 1, then blockchain 2 becomes invalid, the reward of the previous block goes to the miner from blockchain 1 and the

transactions that were part of blockchain 2 and weren't added to the blockchain go back to the transactions pool and get added to the next blocks. In short, if there is a conflict on the blockchain, then the longest chain wins.

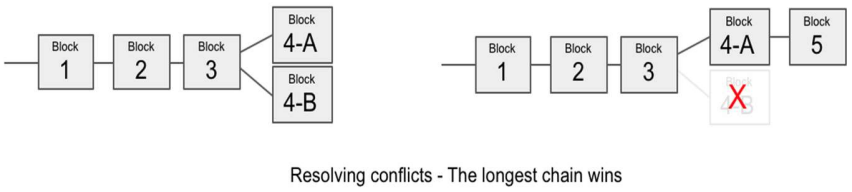

Fig 13: blocks adding

Making your own version of Bitcoin is not that difficult. By utilizing existing technology, implemented in an innovative way, you have everything you need for a cryptocurrency. All transaction is made over the Internet using P2P communication, thus removing the need for a central authority. Users can perform anonymous transactions by utilizing asynchronous cryptography and they are identified only by their private key/public key combination. You have implemented a validated global ledger of all transactions that has been safely copied to every peer in the network. You have a secured, automated, and controlled money supply, which assures the stability of your currency without the need of central authority.

The most popular ways for performing double-spending attacks on the blockchain, and the measures that users should take to prevent damages from them.

5.5 Race Attack

An attacker sends the same coin in rapid succession to two different addresses. To prevent from this attack, it is recommended to wait for at least one block confirmation before accepting the payment.

5.6 Finney Attack

An attacker pre-mines a block with a transaction, and spends the same coins in a second transaction before releasing the block. In this scenario, the second transaction will not be validated. To prevent from this attack, it is recommended to wait for at least 6 block confirmations before accepting the payment.

5.7 Majority Attack (also called 51% attack)

In this attack, the attacker owns 51% of the computing power of the network. The attacker starts by making a transaction that is broadcasted to the entire network, and then mines a private blockchain where he double-spends the coins of the previous transaction. Since the attacker owns the majority of the computing power, he is guaranteed that he will have at some point a longer chain than the "honest" network. He can then release his longer blockchain that will replace the "honest" blockchain and cancel the original transaction. This attack is highly unlikely, as it’s very expensive in blockchain networks like Bitcoin.

CHAPTER 6
IMPLEMENTATION

6.1 PSEUDO CODE

Sending bitcoin money goes as follows:

- Step 1 (one-time effort): Create a bitcoin wallet. For a person to send or receive bitcoins, she needs to create a bitcoin wallet. A bitcoin wallet stores 2 pieces of information: A private key and a public key. The private key is a secret number that allows the owner to send bitcoin to another user, or spend bitcoins on services that accept them as payment method. The public key is a number that is needed to receive bitcoins. The public key is also referred to as bitcoin address (not entirely true, but for simplicity we will assume that the public key and the bitcoin address are the same). Note that the wallet doesn't store the bitcoins themselves. Information about bitcoins balances are stored on the Bitcoin's blockchain.
- Step 2: Create a bitcoin transaction. If Alice wants to send 1 BTC to Bob, Alice needs to connect to her bitcoin wallet using her private key, and create a transaction that contains the amount of bitcoins she wants to send and the address where she wants to send them (in this case Bob's public address).
- Step 3: Broadcast the transaction to Bitcoin's network. Once Alice creates the bitcoin transaction, she needs to broadcast this transaction to the entire Bitcoin's network.

- Step 4: Confirm the transaction. A miner listening to Bitcoin's network authenticates the transaction using Alice's public key, confirms that Alice has enough bitcoins in her wallet (in this case at least 1 BTC), and adds a new record to Bitcoin's Blockchain containing the details of the transaction.
- Step 5: Broadcast the blockchain change to all miners. Once the transaction is confirmed, the miner should broadcast the blockchain change to all miners to make sure that their copies of the blockchain are all in sync.

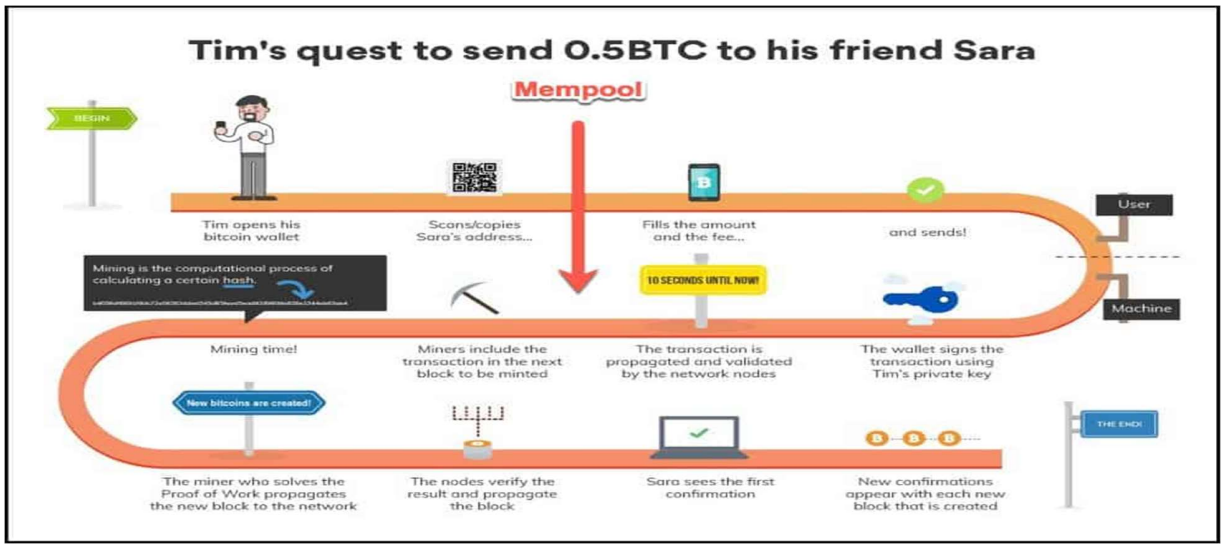

Fig 14: how bitcoin flows:

Our blockchain will have the following features:

- Possibility of adding multiple nodes to the blockchain
- Proof of Work (PoW)
- Simple conflict resolution between nodes
- Transactions with RSA encryption

Our blockchain client will have the following features:

- Wallets generation using Public/Private key encryption (based on RSA algorithm)
- Generation of transactions with RSA encryption

We will also implement 2 dashboards:

- "Blockchain Frontend" for miners
- "Blockchain Client" for users to generate wallets and send coins

The client-side dashboard has 3 tabs in the navigation bar:

- Wallet Generator: To generate wallets (Public/Private keys pair) using RSA encryption algorithm
- Make Transaction: To generate transactions and send them to a blockchain node
- View Transactions: To view the transactions that are on the blockchain
    - We define a python class that we name `Transaction` that has 4 attributes `sender_address`, `sender_private_key`, `recipient_address`, `value`.

      These are the 4 pieces of information that a sender needs to create a transaction.
    - The `to_dict()` method returns the transaction information in a Python dictionary format (without the sender's private key).

      The `sign_transaction()` method takes the transaction information (without the sender's private key) and signs it using the sender's private key.

- The line below initiate a Python Flask app that we will use to create different APIs to interact with the blockchain and its client.

```
app = Flask(__name__)
```

- Below we define the 3 Flask routes that returns html pages. One html page for each tab.

```
@app.route('/')
def index():
  return render_template('./index.html')


@app.route('/make/transaction')
def make_transaction():
    return render_template('./make_transaction.html')


@app.route('/view/transactions')
def view_transaction():
    return render_template('./view_transactions.html')
```

- Below we define an API that generates wallets (Private/Public keys pairs).

```
@app.route('/wallet/new', methods=['GET'])
def new_wallet():
  random_gen = Crypto.Random.new().read
  private_key = RSA.generate(1024, random_gen)
  public_key = private_key.publickey()
  response = {
    'private_key':  binascii.hexlify(private_key.exportKey(format='DER')).decode
('ascii'),
    'public_key':  binascii.hexlify(public_key.exportKey(format='DER')).decode('
ascii')
  }


  return jsonify(response), 200
```

- Below we define an API that takes as input sender_address, sender_private_key, recipient_address, value, and returns the transaction (without private key) and the signature.

```
@app.route('/generate/transaction', methods=['POST'])
def generate_transaction():
```

```
 sender_address = request.form['sender_address']
 sender_private_key = request.form['sender_private_key']
 recipient_address = request.form['recipient_address']
 value = request.form['amount']
 transaction = Transaction(sender_address, sender_private_key, recipient_ad
dress, value)
response = {'transaction': transaction.to_dict(), 'signature': transaction.sign_tr
ansaction()}

 return jsonify(response), 200
```

The front-end user side dashboard has 2 tabs in the navigation bar:

- Mine: For viewing transactions and blockchain data, and for mining new blocks of transactions.
- Configure: For configuring connections between the different blockchain nodes.

Some basic explanation of the code:

- transactions: List of transactions that will be added to the next block.
- chain: The actual blockchain which is an array of blocks.
- nodes: A set containing node urls. The blockchain uses these nodes to retrieve blockchain data from other nodes and updates its blockchain if they're not in sync.

- node_id: A random string to identify the blockchain node.

The Blockchain class also implements the following methods:

- register_node(node_url): Adds a new blockchain node to the list of nodes.
- verify_transaction_signature(sender_address, signature, transaction): Checks that the provided signature corresponds to transaction signed by the public key (sender_address).
- submit_transaction(sender_address, recipient_address, value, signature): Adds a transaction to list of transactions if the signature verified.
- create_block(nonce, previous_hash): Adds a block of transactions to the blockchain.
- hash(block): Create a SHA-256 hash of a block.
- proof_of_work(): Proof of work algorithm. Looks for a nonce that satisfies the mining condition.
- valid_proof(transactions, last_hash, nonce, difficulty=MINING_DIFFICULTY): Checks if a hash value satisfies the mining conditions. This function is used within the proof_of_work function.
- valid_chain(chain): checks if a bockchain is valid.
- resolve_conflicts(): Resolves conflicts between blockchain's nodes by replacing a chain with the longest one in the network.

The line below initate a Python Flask app that we will use to create different APIs to interact with the blockchain.

```
app = Flask(__name__)

CORS(app)
```

Next, we initiate a Blockchain instance.

```
blockchain = Blockchain()
```

Below we define the 2 Flask routes that return the html pages for our blockchain frontend dashboard.

```
@app.route('/')
def index():
    return render_template('./index.html')
@app.route('/configure')
def configure():
    return render_template('./configure.html')
```

Below we define Flask APIs to manage transactions and mining the blockchain.

- '/transactions/new': This API takes as input 'sender_address', 'recipient_address', 'amount' and 'signature', and adds the transaction to the list of transactions that will be added to next block if the signature is valid.
- '/transactions/get': This API returns all the transactions that will be added to the next block.

- '/chain': This API returns all blockchain data.
- '/mine': This API runs the proof of work algorithm, and adds the new block of transactions to the blockchain.

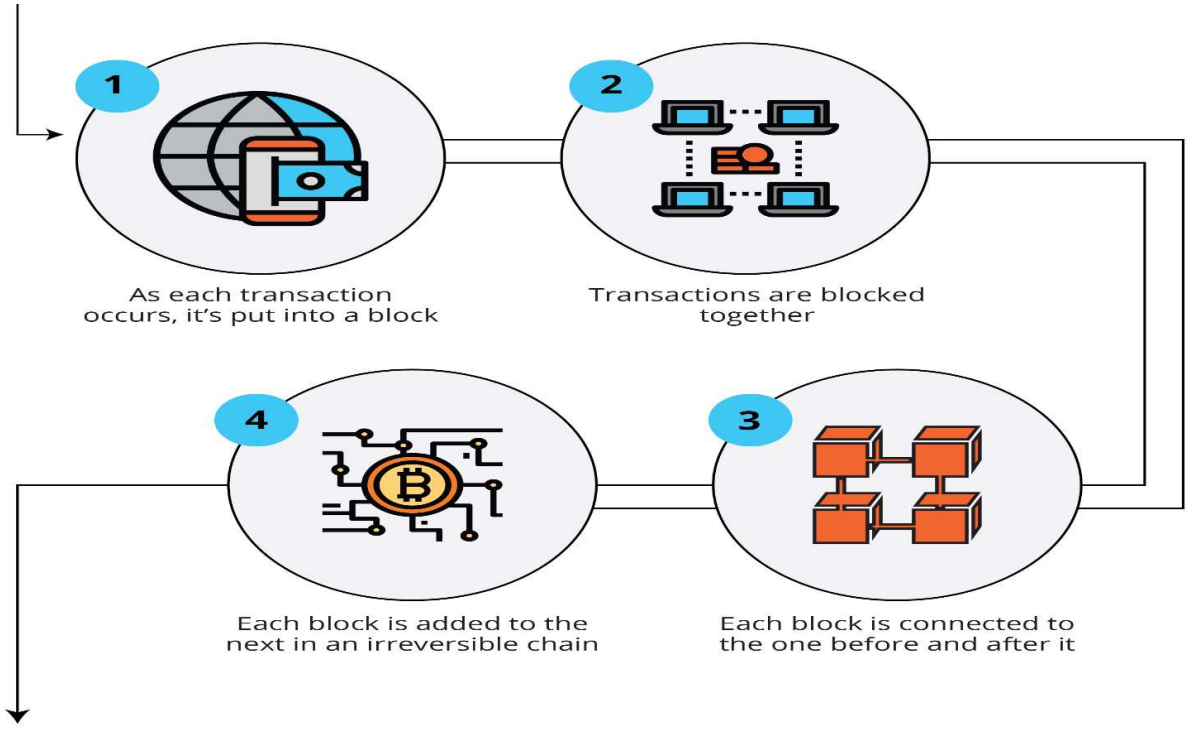

Fig 15: Implementation

CHAPTER 7
RESULT ANALYSIS

- There should be previous knowledge of some security algorithms and attacks before studying this system:

1. RSA
2. Digital Signature
3. Hashing algorithm
4. Adding blocks to chain
5. Peer to peer network
6. Double spending

- Making your own version of Bitcoin is not that difficult. By utilizing existing technology, implemented in an innovative way, you have everything you need for a cryptocurrency.
- All transaction is made over the Internet using P2P communication, thus removing the need for a central authority
- Users can perform anonymous transactions by utilizing asynchronous cryptography and they are identified only by their private key/public key combination
- You have implemented a validated global ledger of all transactions that has been safely copied to every peer in the network

- You have a secured, automated, and controlled money supply, which assures the stability of your currency without the need of central authority

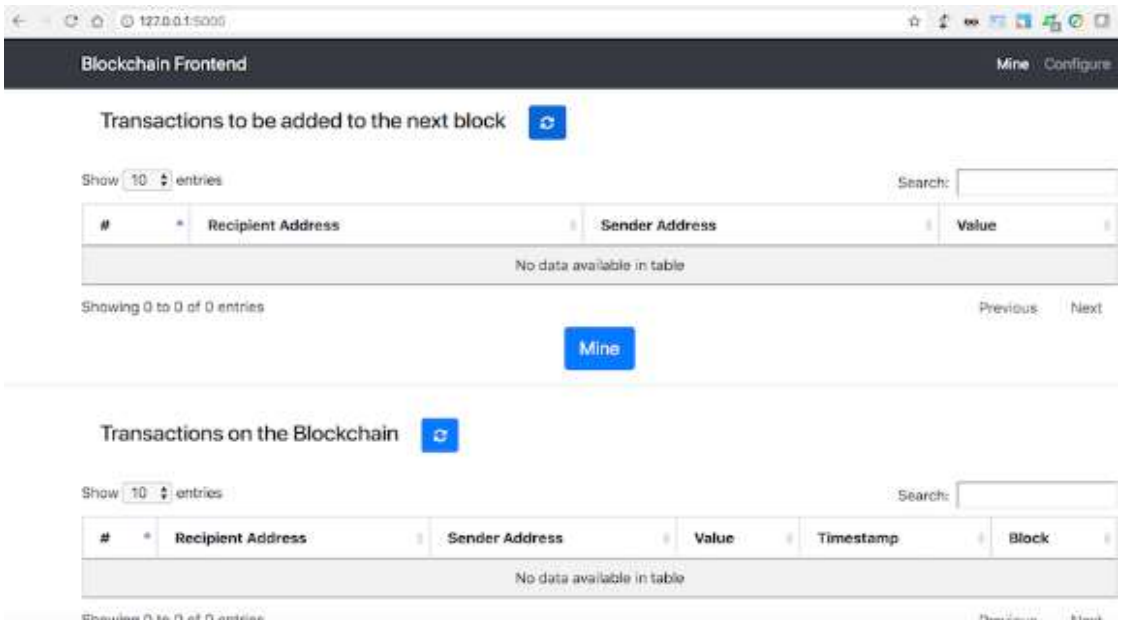

Fig 16: FRONTEND-SIDE IMPLEMENTATION

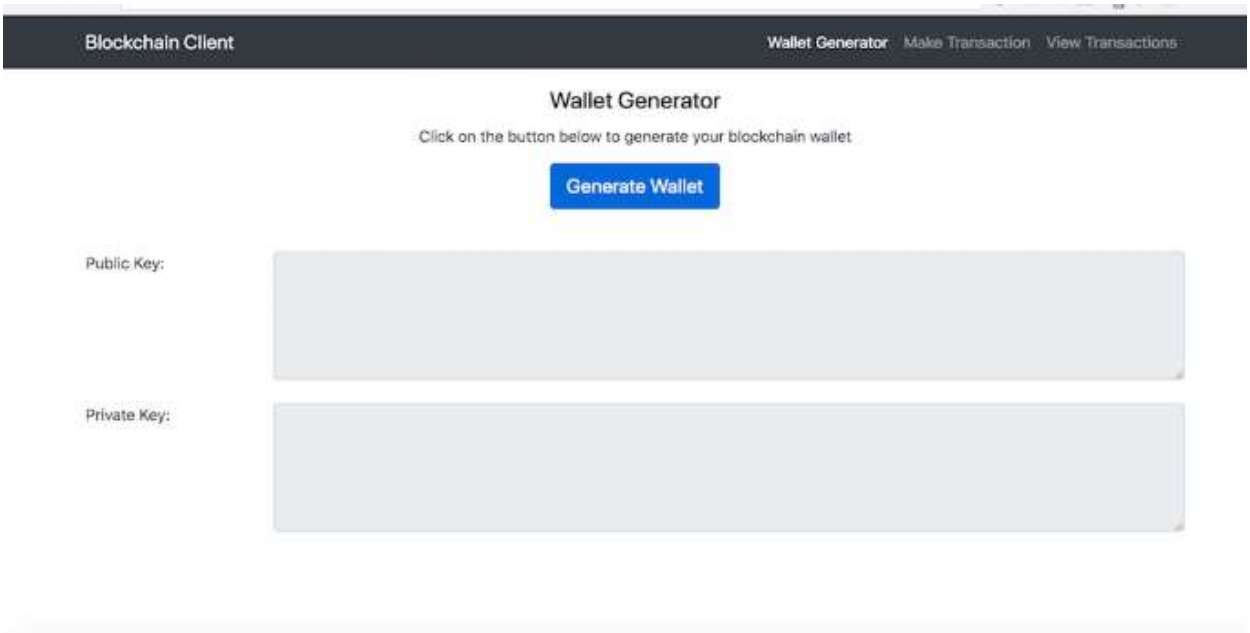

Fig 17: CLIENT-SIDE IMPLEMENTATION

7.1 Applications of Blockchain:

- Government
- Healthcare
- Banking
- Real estate
- Travel
- Food and supply chain
- Automotive
- Security
- Agriculture
- Education
- Insurance
- Retail and consumer products

Fig 18: Application of blockchain.

7.2 USES OF BLOCKCHAIN:

Bank Use

Perhaps no industry stands to benefit from integrating blockchain into its business operations more than banking. Financial institutions only operate during business hours, five days a week. That means if you try to deposit a check on Friday at 6 p.m., you likely will have to wait until Monday morning to see that money hit your account. Even if you do make your deposit during business hours, the transaction can still take one to three days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps. By integrating blockchain into banks, consumers can see their transactions processed in as little as 10 minutes, basically the time it takes to add a block to the blockchain, regardless of the time or day of the week. With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely. In the stock trading business, for example, the settlement and clearing process can take up to three days (or longer, if banks are trading internationally), meaning that the money and shares are frozen for that time. Given the size of the sums involved, even the few days that the money is in transit can carry significant costs and risks for banks. Santander, a European bank, put the potential savings at $20 billion a year. Capgemini, a French consultancy, estimates that consumers could save up to $16 billion in banking and insurance fees each year through blockchain-based applications.

Use in Cryptocurrency

Blockchain forms the bedrock for cryptocurrencies like Bitcoin. As we explored earlier, currencies like the U.S. dollar are regulated and verified by a central authority, usually a bank or government. Under the central authority system, a user's data and currency are technically at the whim of their bank or government. If a user's bank collapses or they live in a country with an unstable government, the value of their currency may be at risk. These are the worries out of which Bitcoin was borne. By spreading its operations across a network of computers, blockchain allows Bitcoin and other cryptocurrencies to operate without the need for a central authority. This not only reduces risk but also eliminates many of the processing and transaction fees. It also gives those in countries with unstable currencies a more stable currency with more applications and a wider network of individuals and institutions they can do business with, both domestically and internationally (at least, this is the goal.)

Healthcare Uses

Health care providers can leverage blockchain to securely store their patients' medical records. When a medical record is generated and signed, it can be written into the blockchain, which provides patients with the proof and confidence that the record cannot be changed. These personal health records could be encoded and

stored on the blockchain with a private key, so that they are only accessible by certain individuals, thereby ensuring privacy

Property Records Use

If you have ever spent time in your local Recorder's Office, you will know that the process of recording property rights is both burdensome and inefficient. Today, a physical deed must be delivered to a government employee at the local recording office, where is it manually entered into the county's central database and public index. In the case of a property dispute, claims to the property must be reconciled with the public index. This process is not just costly and time-consuming—it is also riddled with human error, where each inaccuracy makes tracking property ownership less efficient. Blockchain has the potential to eliminate the need for scanning documents and tracking down physical files in a local recording office. If property ownership is stored and verified on the blockchain, owners can trust that their deed is accurate and permanent.

Use in Smart Contracts

A smart contract is a computer code that can be built into the blockchain to facilitate, verify, or negotiate a contract agreement. Smart contracts operate under a set of conditions that users agree to. When those conditions are met, the terms of the agreement are automatically carried out. Say, for example, I'm renting you my apartment using a smart contract. I agree to give you the door code to the apartment

as soon as you pay me your security deposit. Both of us would send our portion of the deal to the smart contract, which would hold onto and automatically exchange my door code for your security deposit on the date of the rental. If I don't supply the door code by the rental date, the smart contract refunds your security deposit. This eliminates the fees that typically accompany using a notary or third-party mediator.

Supply Chain Use

Suppliers can use blockchain to record the origins of materials that they have purchased. This would allow companies to verify the authenticity of their products, along with health and ethics labels like "Organic," "Local," and "Fair Trade." As reported by Forbes the food industry is moving into the use of blockchain to increasingly track the path and safety of food throughout the farm-to-user journey.

Uses in Voting

Voting with blockchain carries the potential to eliminate election fraud and boost voter turnout, as was tested in the Nov. 2018 midterm elections in West Virginia. Each vote would be stored as a block on the blockchain, making them nearly impossible to tamper with. The blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct an election and provide officials with instant results.

CHAPTER-8
CONCLUSION AND FUTURE SCOPE

We hope our trained cascade can be used in some applications such as intelligent searching. which searches for eyes and mouth through horizontal and vertical overlapping blocks of the edge image. In the future it will be very affected.

8.1 CONCLUSION

Blockchain is the technology which is expected to grow very vastly in the near future. No doubt there has been a downfall in this service people has dropped their funds for blockchain but for the ones who wishes to invest in it can have a benefit in multiples of the number. Reading the above paragraphs, it is quite clear that blockchain has many advantages and it can likely improve our lifestyle. Every advancement come with some disadvantages too but it is expected to find out some better ways to eliminate the risk and make more popular between the business societies. So, I studied many implementations from previous works and tried it to understand the way how crypto mining works and how bitcoin works. This report includes all the information about blockchain, from its definition to its advantages and disadvantages including application and how does it work. After that it concludes about crypto mining and my implementation of bitcoin in it. Summarily, a detailed explanation is there about how can you make your own money, how to

send bitcoin, its lifetime to how it works. Blockchain truly has the potential to become the next big thing in technology space and when it matures, much like what internet did in the 1990s, it can disrupt several industries at scale. As we have seen, firms across several industries have already started adopting and piloting a few internal services on Blockchain. So, how fast the technology gains mass adoption is now a function of how rapidly innovative applications can be built on top of Blockchain. Cryptocurrencies such as Bitcoin, on the other hand, although popular, may take some time to be adopted as a primary medium of exchange, replacing fiat currencies. We have already seen how Bitcoin standard is seen in comparison to the Gold standard, without some of the disadvantages of the latter. To become the future currency of the world, it needs to get the nod of governments and policy makers. It also needs to make itself technologically much safer to vulnerable attacks. These are as much a problem of public perception as they are about the economic soundness. In the truly exciting times ahead, we only have to wait and watch how Bitcoins and Blockchain play out and where they live up to their potential and promises.

8.2 FUTURE SCOPE

Blockchain technology has a great future worldwide. An incredible scope of Blockchain technology has been observed in the financial field. The financial organizations were not able to sufficiently handle the heavy workload after

demonetization and thus brought out the problems of having a centralized specialist for handling the financial transactions. As a result, the RBI is inspiring banks to encourage digitization. They have also released a statement which emphasized the probability of Blockchain to fight faking and the chances of bringing about particular modifications in the working of financial markets, collateral identification and payment system. Incorporating Blockchain with financial transactions gives out amazing benefits, such as a significant amount of time and money could be saved, including a drastic reduction in time needed for processing and validating transactions. The blockchain functions on a distributed database which make the operations smoothly, ensuring tight security, and made it safe from cyber-attacks.

After recognizing the benefits of Blockchain Technology, several financial institutions have started spending considerably in this particular field. Blockchain can also help in shortening the flow of black-money and dealing with the extensive money cleaning in the economy because each address used for transactions is stored forever on the databases, making all the transactions provable and responsible. The government is observing Blockchain as a way to explore a range of options which may help to apply a fitter control on the nation's economy.

Blockchain Technology is one of the most consistent technologies when it requires to keep track of financial properties. Blockchain technology has attracted many companies who want to add the distinct features of it to their security structures.

Many studies have been carried out for digital currencies and blockchain technology, which represents that both of these technologies will be continuing to disrupt the world.

Apart from financial industries, blockchain technology also has a bright future in other sectors. Let us have a look at the future scope of Blockchain technology in different sectors:

1. Blockchain in Digital Advertising: Presently, digital advertising faces a lot of challenges like domain fraud, bot traffic, lack of transparency and long payment models, due to the issue like incentives are not affiliated. Because of this the promoters and publishers feel they are dropping the deal. Blockchain has provided a solution to carry transparency to the supply chain as it fetches trust in a trustless environment. Blockchain allows right companies to succeed, by decreasing the number of bad players in the supply chain. Publishers can also gather a vast percentage of the total advertisement dollars arriving the ecosystem. The Blockchain technology is still in its beginning; however, this technology should stay here, and all advertisement companies are observing that how blockchain will help to enhance their business.

2. Blockchain in Cyber Security: Though the blockchain is a public ledger, the data is verified and encrypted using innovative cryptography technology. In this manner, the information or data is less likely to be attacked or altered without authorization.

3. Blockchain will remove the requirement of the third party: With the help of Blockchain technology, basically, it is possible to impact a varied range of processes and techniques. It eliminates the need of trusted third party in the transactions. Well most prominent organizations in the world exist today to function as a trusted third party, for instance, SWIFT, and the Depository Trust Cleaning Company. Corporate chances flourish for companies that can build applied Blockchain technologies aiming for particular transactions, like the mortgage industry. The existing mortgages needed a complicated web of title searches, title insurance, and uncountable minor transaction fees which are required to keep the system running. These systems occur because traditionally, the transfer of land has been a process which requires a significant amount of belief in the old records. The Blockchain technology was going to address all these concerns, and a particular property's ledger consists of a verifiable and validated transactions history, lowering the necessity of institutions to provide risk modification and trust services.

4. Governments will provide their digital currencies: It is confirmed that the paper money at its last phase, but it is also found that the authorized currency is facing a severe competition by cryptocurrencies. In 2017, it is observed that the price of Bitcoin has flown which was never seen by any single service or money all around the world. The currency is still one of the most appreciated properties available in the market, and the nation took notice, due to the price of Bitcoin is denied by the

basic idea of demand and supply. The need for Bitcoin will again climb at some point, with a fixed limit of twenty-one million units of Bitcoin. Because of this, a few governments will get a chance to create their digital currencies to avoid dropping face to an independent and unregulated property and participate in an open market.

5. Blockchain beyond the world of computing: In 2017, the world had seen the infinite collection of options in the use of blockchain technology. Currently, most of the countries are developing their blockchain strategies to hold the future. Also, it is highly possible that the rest of the advanced European countries will follow suit by accepting the blockchain technology to create a constant financial environment that helps nations on ruins like Greece and Spain. There are specific problems associated with the security of finances, and Blockchain will be used to address these kinds of issues. Blockchain will also be used to generate registries which are used for medical purposes, to manage insurance policies, and to interrupt the model of useless data storage.

6. Managing World trade with the help of Blockchain Technology: Blockchain is valuable to business particularly how it makes easy for anybody to track the supply chain of everything provided using the technology. It will be outdated to track the numbers, and no company wants to lose a shipment because of human inability. Well, it is easy to register a cargo shipment in the Blockchain, this enables the parties involved in the job operation to follow the delivery procedure from point A to B.

With the help of Blockchain technology, it is easy for the custom agents to track down the forbidden products like fake medicines, changed food products, false clothes reproduction, fake auto parts, electronic apparatus and other piracy agents which are trying to provide the low-quality goods inside any country without talking about the internal laws.

7. Supply chain Management: With the help of blockchain technology, it is possible to document the transaction in an everlasting distributed record, and supervise the transactions more sturdily and transparently. This also helps to minimize human errors and time delays. It is also used monitor costs, employment, and releases at each point of the supply chain. But this has severe effect for understanding and monitoring the actual ecological impacts of products. Not only this the decentralized ledger can also be utilized to check the legitimacy or fair trade status of products by following them form their source.

8. The Blockchain in Forecasting: The blockchain technology is set to alter the complete methodology for research, consulting, analysis and forecasting. The global distributed prediction markets are created with the help of online platforms.

9. Use of Blockchain in the Internet of Things and Networking: Different companies like Samsung and IBM are utilizing the blockchain technology for a new concept called ADEPT, this will help to create a distributed network of IoT devices. The blockchain technology will remove the requirement for a central location to manage

the communication between them; this will function as a public ledger for a massive number of devices. The devices may communicate with each other to upgrade the software, handle the errors and observe energy practice.

10. Blockchain in cloud storage: The data on a centralized server is exposed to hacking, loss of data, or human error. With the help of blockchain technology, it is possible to make the cloud storage more protected and robust against hacking.

8.3 REFERENCES:

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf [Accessed: 8 May 2018].

[2] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and Cryptocurrency Technologies. Princeton University Press, 2016, 308 p.

[3] G. Hileman & M. Rauchs, Global Blockchain Benchmarking Study. Cambridge, United Kingdom: Cambridge Centre of Alternative Finance, Sept. 2017. Available: https://ssrn.com/abstract=3040224 [Accessed:8 May 2018].

[4] D. Yang, J. Gavigan, and Z. Wilcox-O'Hearn, Survey of Confidentiality and Privacy Preserving Technologies for Blockchains, 2016.Available: https://www.r3.com/wp-content/uploads/2017/06/survey_ confidentiality_privacy_R3.pdf [Accessed: 8 May 2018].

[5] Citi Group. [Online]. Citi GPS: How FinTech is Forcing Banking to a Tipping Point, March 2016. Available: https://www.citivelocity.com/citigps/ [Accessed: 3 May 2018].

[6] Everis NEXT, "17 Blockchain Disruptive Use Cases," 31 May 2016. [Online]. Available: https://everisnext.com/2016/05/31/blockchain-disruptive-use-cases/ [Accessed: 8 May 2018].

[7] R. Krawiec, D. Housman, M. White, M. Filipova, F. Quarre, D. Barr, A. Nesbitt, K. Fedosova, J. Killmeyer, A. Israel, and L. Tsa, Blockchain: Opportunities for Health Care. NIST Workshop on Blockchain & Healthcare, Aug. 2016. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us blockchain-opportunities-for-health-care.pdf [Accessed: 8 May 2018].

[8] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A Systematic Literature Review," in IEEE/ACS 13th International Conference of Computer Systems and Applications, 2016, pp. 1–6. https://doi.org/10.1109/AICCSA.2016.7945805

[9] "Survey on Establishing Evaluation Model for Blockchain," Mitsubishi Research Institute, 2017. Available: http://www.meti.go.jp/meti_lib/report/H28FY/000346.pdf [Accessed: 8 May 2018].

[10] P. Zhang, D. C. Schmidt, J. White, and G. Lenz, "Metrics for Assessing Blockchain-Based Healthcare Decentralized Apps," in IEEE 19th International Conference on e-Health Networking, Applications and Services, 2017 pp. 17–20. https://doi.org/10.1109/HealthCom.2017.8210842

[11] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in IEEE 6th International Congress on Big Data, June 2017, pp. 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

[12] N. Bauerle, "What are the Applications and Use Cases of Blockchain?". [Online]. Available: https://www.coindesk.com/information/applications-use-cases-blockchains [Accessed: 8 May 2018].

[13] K. Christidis and M. Devetsikioti, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016. https://doi.org/10.1109/access.2016.2566339

[14] BitFury Group and J. Garzik, "Public versus Private Blockchains — Part1: Permissioned Blockchains, Part2: Permissionless Blockchains,2015. Available: http://bitfury.com/docs/

[15] V. Lemieux, Blockchain Technology for Record Keeping: Help or Hype?, vol 1. University of British Columbia, 2016. Available: https://www.researchgate.net/profile/Victoria_Lemieux [Accessed: 8 May 2018].

[16] H. Okada, S. Yamasaki, and V. Bracamonte, “Proposed Classification of Blockchains Based on Authority and Incentive Dimensions,” in 19th International Conference on Advanced Communication Technology, 2017. https://doi.org/10.23919/ICACT.2017.7890159

[17] B. A. Tama, B. J. Kweka, Y. Park, and K. H. Rhee, “A Critical Review of Blockchain and Its Current Applications,” in International Conference on Electrical Engineering and Computer Science, 2017, pp. 109–113. https://doi.org/10.1109/ICECOS.2017.8167115

[18] A. Lewis, “So You Want to Use a Blockchain for That?,” Jul. 2016. [Online]. Available: https://www.coindesk.com/want-use-blockchain/ [Accessed: 8 May 2018].

[19] H. Halpin and M. Piekarska, “Introduction to Security and Privacy on the Blockchain,” in 2nd IEEE European Symposium on Security and Privacy Workshops, 2017. https://doi.org/10.1109/EuroSPW.2017.43

[20] S. Porru, A. Pinna, M. Marchesi, and R. Tonelli, “Blockchain-Oriented Software Engineering: Challenges and New Directions,” in IEEE 39th International Conference on Software Engineering Companion, May 2017, pp. 169–171. https://doi.org/10.1109/ICSE-C.2017.142

[21]. Perea, R.G.; Garcia, I.F.; Arroyo, M.M.; Diaz, J.A.R.; Poyato, E.C.; Montesinos, P. Multiplatform application

[22]. Yu, Q.Y.; Shi, Y.; Tang, H.J.; Yang, P.; Xie, A.K.; Liu, B.; Wu, W.B. eFarm: A tool for better observing agricultural land systems. Sensors 2017, 17. [CrossRef] [PubMed]

[23]. Jiang, J.A.; Wang, C.H.; Liao, M.S.; Zheng, X.Y.; Liu, J.H.; Chuang, C.L.; Hung, C.L.; Chen, C.P. A wireless sensor network-based monitoring system with dynamic converge cast tree algorithm for precision cultivation management in orchid greenhouses. Precis. Agric. 2016, 17, 766–785. [CrossRef]

[24]. Lin, Y.P.; Chang, T.K.; Fan, C.; Anthony, J.; Petway, J.R.; Lien, W.Y.; Liang, C.P.; Ho, Y.F. Applications of information and communication technology for improvements of water and soil monitoring and assessments in agricultural areas—A case study in the taoyuan irrigation district. Environments 2017, 4, 6. [CrossRef]

[25]. Yoshida, K.; Tanaka, K.; Hariya, R.; Azechi, I.; Iida, T.; Maeda, S.; Kuroda, H. Contribution of ict monitoring system in agricultural water management and environmental conservation. In Serviceology for Designing the Future; Springer: Tokyo, Japan, 2016; pp. 359–369.

[26]. Jagannathan, S.; Priyatharshini, R. In Smart farming system using sensors for agricultural task automation. In Proceedings of the IEEE Technological Innovation in ICT for Agriculture and Rural Development (TIAR), Chennai, India, 10–12 July 2015; pp. 49–53.

[27]. Bartlett, A.C.; Andales, A.A.; Arabi, M.; Bauder, T.A. A smartphone app to extend use of a cloud-based irrigation scheduling tool. Comput. Electron. Agric. 2015, 111, 127–130. [CrossRef]

[28]. Adil, A.; Badarla, V.; Plappally, A.K.; Bhandari, R.; Sankhla, P.C. Development of affordable ICT solutions for water conservation in agriculture. In Proceedings of the 7th International Conference on Communication Systems and Networks (COMSNETS), Bangalore, India, 6–10 January 2015; pp. 1–6.

[29]. Abbasi, A.Z.; Islam, N.; Shaikh, Z.A. A review of wireless sensors and networks' applications in agriculture. Comput. Stand. Interfaces 2014, 36, 263–270.

[30]. Gebbers, R.; Adamchuk, V.I. Precision agriculture and food security. Science 2010, 327, 828–831. [CrossRef] [PubMed]