APPLICATION OF BLOCKCHAIN TECHNOLOGY

For Transforming Indian Economy

BY AMAN DUBEY

Last updated: September 02, 2019

The information contained in this book is for general information purposes only .Author assumes no responsibility for errors or omissions in the contents. In no event shall Author be liable for any special, direct, indirect, consequential, or incidental damages or any damages whatsoever, whether in an action of contract, negligence or other tort, arising out of or in connection with the use of the Service or the contents of the Service. Author reserves the right to make additions, deletions, or modification to the contents on the Service at any time without prior notice.

TABLE OF CONTENTS

Contents

LIST OF ABBREVIATIONS

• OS	Operating system
• ICO	Initial Coin Offering
• AI	Artificial Intelligence
• P2P	Peer To Peer
• ADMIN	Administrator
• ID	Identity
• DILRMP	Digital India Land Records Modernization Programme
• PKI	Public Key Infrastructure
• UETP	Uniform Economic Transaction Protocol
• CV	Curriculum Vitae
• IRDAI	Insurance Regulatory and Regulation Authority of India
• GEC	General Insurance Company
• FIR	First Response Copy
• FDI	Foreign Direct Investment
• FY	Financial Year
• RFID	Radio Frequency Identification
• MNC	Multi National Company
• INR	Indian Rupee
• PIN	Personal Identification Number
• NITI	National Institute for Transforming India
• E-VOTING	Electronic Voting
• E-GOVERNAMCE	Electronic Governance
• CAGR	Compound Annual Growth Rate
• UNDP	United Nations Development Programme
• ICT	Information and Communications Technology
• PHI	Protected Health Information
• WHO	World Health Organization
• HIPAA	Health Insurance Portability and Accountability Act

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

CHAPTER – 1

Key Topics Discussed in this Chapter

- Introduction
- History of Blockchain
- Review of Literature
- Statement Of Problem
- Research Questions
- Research Objectives
- Scope Of Study
- Research Tool
- Research Methodology

1.1.Introduction

Blockchains are incredibly popular nowadays. What is a Blockchain? How do they work? What problems are they solve and how can they be used? As the name indicates a Blockchain is a series of blocks contains permissions. This technique was originally described in 1991 when research scientists, introduced that computationally practical solutions for timestamping digital documents. So that they could not back data or tempered with the system, use the cryptographic list, secure chain of blocks to store the timestamped document. It allows every client and the network to reach consensus without ever having to trust each other is the idea behind Blockchain. In 2009, to create a digital cryptocurrency, Bitcoin and Blockchain as a distributed ledger come in the picture, if some data has been recorted inside the Blockchain. It becomes very difficult to change it. So, how does that work? Well, let's take a closer look at a block. Each block contains some data hash of the block, the previous block and the data that is stored inside the block is depends on the type of Blockchain, in case of the Bitcoin Blockchain stores the details about a transaction such as the sender, receiver and the amount. Once hash is created its hashes being calculated changing something inside the block will also cause the hash to change. So, in other words, hashes are very

useful when you want to detect changes to block it can be consider as a fingerprint which is unique for each entity. If the fingerprint of a block changes, it no longer is the same block. The third

element inside each block is the hash of the previous block. And this effectively creates the chain of blocks therefore, this technique that makes the Blockchain so secure. For better understanding Let's take an example of a chain of three blocks (BLOCK 1, BLOCK2 AND BLOCK 3). Each block has hashed and the hash of the previous block. So blocked number three points to block number two and number two points to number one. The first block is a bit special. It kind of points of previous blocks because well, it's the first one we call this block, the genesis block now, let's say that in tamper with the second block, this causes the hash of the block, the changes well, intern, that will make block three and all following blocks invalid, because they no longer store a valid hash of the previous block. So changing a single block will make all following blocks invalid but using hashes is not enough to prevent tampering. Computers these days are very fast and can calculate hundreds of thousands of hashes per second. You could effectively tamper with a block and recalculate all the hashes of other blocks to make Blockchain valid again. So to mitigate this Blockchain has something that is called Proof of work. It's a mechanism that slows down the creation of new blocks in Bitcoins case it takes about ten minutes to calculate the required proof of work and add a new block to the chain.

This mechanism makes it very hard to tamper with the blocks because if you are tampering with one block you have to recalculate the proof of work for all blocks. So, the security of the Blockchain comes from its creative use of hashing and the proof of mechanism, but there is one more way that Blockchain securing themselves, and that is by being distributed. Instead of using the central entity to manage the chain, Blockchain uses a peer to peer network and anyone is allowed to join.

When someone joins this network, he gets a full copy of the Blockchain. The node can use this to verify that everything is still in order. Now let's see what happens when someone creates a new block, the new block is sent to everyone on the network. Each node then verifies the block to make sure that it hasn't been tampered with and if everything checks out each node adds this block to their own Blockchain. All the notes in this network create consensus, they agree about what blocks are valid and which aren't. Blocks that are tempered with will be rejected by other nodes in the network. So to successfully tamper with the Blockchain, you'll need to tamper with all the blocks on the chain, redo the proof of work for each block and take control of more than fifty percent of the peer to peer network. Only then, your tempered block become accepted by everyone else so this is almost impossible to do. Blockchains are also constantly evolving.

One of the most recent developments is the creation of smart contracts. These contracts are simple program that are stored on the Blockchain. It can be used to automatically exchange coins based on certain conditions. The creation of Blockchain technology peaked a lot of people's interest.

Soon others realized that this technology can be used for other things like storing medical records, creating a digital notary or even collecting taxes. So now, you know what a Blockchain is how it works on the basic level and what problems it solves.

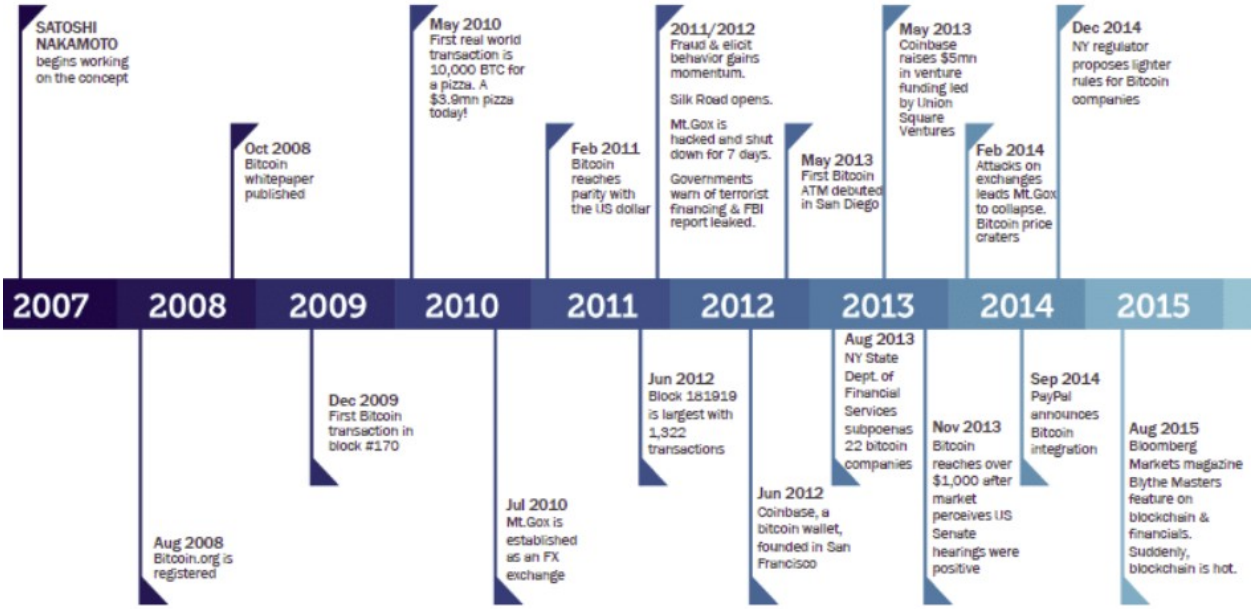

Figure 1: Blockchain History

1.2. History of Blockchain

- Blockchain may sound like a new idea, but there's a rich history of innovation that led up to Satoshi Nakamoto creation of the first Blockchain Bitcoin in 2009.
- The first mention of any sort of a block chain like technology dates back in 1991, when Stuart Haber and W. Scott Stornetta did the first work on a secured chain of blocks.
- They next year 1992, see the introduction of Merkle trees to block chain-like design which enables multiple documents to be stored within a single block increasing Blockchain efficiency.
- Ten years later in 2002 the concept of decentralized trust with in a network file system was formulated by David Mazieres and Dennis Shasha.

- In 2005, Nick Szabo proposed Bitgold a protocol for decentralized property titles that incorporated a Blockchain-like system. This protocol involved proof of work and timestamping features. Unfortunately, Bitgold has one fatal weakness. It is discovered if

  someone who has the balance of Bitgold could spend their coin twice without being caught. This became known as the "double spending problem"
- Everything mentioned till this point laid to the foundation for the first real Blockchain. While Haber, Stornetta, Mazieres, Szabo were flirting with the idea of a Blockchain, the first real live Blockchain would not be invented until 2008.
- In 2008 Satoshi Nakamoto published a paper called Bitcoin a peer to peer electronic cash system. This paper solve a double spending problem that was seen in bitgold and became the white paper written for the world's first real working Blockchain.
- In 2009 with the help of programmer Hal Finney and others, Nakamoto made Bitcoin a reality.
- The code is written the Blockchain was born and Nakamoto mined the first blocks himself. Hal Finney was a recipient of the very first bitcoin transaction when he received 10 Bitcoin from Nakamoto.
- The years following bitcoins release saw tremendous popularity and use. It became seen a legitimate method of payment. In fact, it was the only one that can be used for certain purposes like donating to WikiLeaks.
- From 2009 to present we've seen huge increases in the file size on a block chains, innovation to the way they work and booms in the price of the shares of the technology. Many people who are uninformed about Blockchain technology think the big coin and Blockchain are the same thing. This is not correct. Actually, Bitcoin as a cryptocurrency protocol built on a Blockchain.
- 2014 was the first year that investors and innovators really started focusing on block chain technology and building new Blockchains.
- In 2014 the term Blockchain 2.0 was first used in the Economist magazine. Blockchain2.0 refers to the emergence of applications that can be executed on a Blockchain database. This innovation represented a massive step forward in the Blockchain technology. With this

concept the prospect of running decentralized apps on a Blockchain became a possibility and smart contracts became plausible as well.

- Very next year, 2015, saw a launch of the first Blockchain 2.0. Vitalik Buterin,a contributor during bitcoins creation saw room for improvement over Bitcoin and wrote code for Etherium. Etherium promises to provide the same functionality as Bitcoin but will also feature the ability to run decentralized apps. While new Blockchain based projects have been emerging since investors and innovators started focusing on Blockchain technology in 2014.
- 2017 was a year marked by an explosion and of Blockchain based platforms. Initial coin offerings also known as ICOs when investors are given the opportunity to buy the first shares in a project became extremely common in 2017.
- Today there are thousands of projects are using Blockchain technology where it goes from here, though, is anybody's guess. In the crypto world knowledge is power and the information is vital.

CHAPTER 2

BLOCKCHAIN OVERVIEW

CHAPTER- 2

Key Topics Discussed in this Chapter

- Blockchain Technology
- Function Component of Blockchain
- Overview
- Benefits of Decentralized system
- Working of Blockchain Technology
- Classification of Blockchain Ledger
- Example of Blockchain Application

2.1. Blockchain Technology

The Blockchain is an astonishing technology that has gained tremendous attention in recent years when the stats of Bitcoin reached a startling height of 17,900$. After the internet, Blockchain is that technology that has the potential which can change our day to day activities.

We have been a victim of Internet that totally changes the way in which we do business, money transfer or contact a person sitting at an immeasurable distance from us. We are moving towards a world of virtual cyberspace and artificial intelligence system exist. This technology revolution needs some more advancements in terms of secure and fast protocols that can add support to the existing system of applications. The Blockchain is the new technology that can hold the burden of technology expansion.

Blockchain or the distributed and secure ledger system has been a matter of discussion since 2008 when Satoshi Nakamoto introduced this technology in his research paper.[1] Till now many researches have been done over its uses and applications. But the reality is, for most of the people

[1] https://www.coindesk.com/information/who-is-satoshi-nakamoto

Blockchain and bitcoin is the same technology with different names. In this paper, we will discuss this technology from ground zero.

The success of bitcoin has started the new era of Blockchain technology. People begin to trust on these virtual currencies. But how many of them know the real concept behind the bitcoin? Let me ask a simple question, did you know how digital currencies works?

If I am not wrong, a large number of the population didn't know the actual difference between the bitcoin and Blockchain. For most of us, bitcoin is equal to a Blockchain. But the reality is far ahead of their thinking. In this paper, we will talk about the Blockchain and discuss how this technology giving the new dimension to the world's existing technical system. Firstly, we will see how bitcoin and Blockchain are two different concepts. The only similarity between them is bitcoin is the application of Blockchain.

For layman introduction to technical background this might be some trouble to understand, let us take an example of your smartphone. Everyone owns an android phone. And you might be using many varieties of application that runs on your android OS like browser, video player, gallery etc. Now relate this concept with Blockchain and bitcoin.

I think you got my point right, If not, let me clear this, like your smartphones have Android OS which is supplemented by some application of your preferences and requirements. In the same way, Blockchain is the technology which is the backbone of different application and the most common application of Blockchain is cryptocurrency. There are many others applications of Blockchain which will be discussed in later part. Now, coming to the working of the Blockchain.

2.2. Functional component of Blockchain system

a. **Nodes**- Node is the smallest unit in this system, every individual who is participating in the network is termed as a node.
b. **Block**- A block is a time-bound unit of data. It stores file or information about the transaction happened in the network. It can relate to a page of a ledger.
c. **Chain**- It is the collection of different blocks that are connected together forming a chain-like structure. Each block connected to a previous block through a mathematical hash function which creates trust between them.
d. **Networks**- Several nodes together form a network. In a network of nodes, each node is connected to every other node. Two nodes can interact with each other whenever they need to. No node outside the network is eligible to participate in the transaction.
e. **Ledger**- A ledger is a record book, where the log has been added of each transaction in a network. All the nodes have their own ledger which stores transactional information that is same for everyone participating in the network.

2.3. Blockchain technology overview

Before coming directly to the Blockchain technology lets discuss why there was a need of this technology so that we may better understand the demand of this system.

The very impressive fact of Blockchain technology is that it solves the very known two problems of currency based transaction i.e Byzantine Generals' Problem and the Double Spend Problem.[2]

Let us take a real-world example of the issues which were faced by the existing technology. All of us use internet banking or at least have used once in a life. Whenever we have to transfer money to someone first we need to contact the bank and then proceed for the request of fund transfer, bank takes your request and then transfer the money to another person's account. All of this process takes about 2 to 3 working days. Also, bank charges some fees for their involvement in this process.

[2] Available at https://coinsutra.com/bitcoin-double-spending/ accessed on 20/10/18

The problem with this system is that we can't transfer money instantly. Also, why would anyone want to give commission to the bank, I am the guy who wants to send money to someone so why shouldn't I directly transfer that money without the involvement of the bank?

The Blockchain is the technology that eliminates the involvement of third party that is a mediator for carrying out any transaction. Blockchain provides peer to peer connection between different nodes. Also, it is a decentralized technology. Here decentralized means there is no kind of central organization government or community who controls, regulates and manages the Blockchain. In Blockchain, there are different computers connected to each other within that network and these computers are known as nodes. We have discussed earlier, Blockchain is the decentralized technology so data is not stored in a central database. In fact, each node has their own record which is same for all.

2.4. Benefits of decentralized system

The problem with the centralized system was that if somehow anyone is able to get access to the main database he can easily steal, delete or modify the repository. If not any other third person is able to get the access to it, Admin or the person who owns that database system can do the same for their personal advancements and this can be the problem of internal threat. Another benefit is, we have eliminated the concept of single point of failure.[3] Suppose a situation where you have to buy anything through an online marketplace or have to transfer some money to your friend's account but due to some technical issue service provider's website is down or not working due to some kind of failure in their system or maybe their website is under a cyber attack. You know how irritating this is. As there is a central database system so if something happens wrong to it, causing great trouble.

[3] Available at https://www.singlegrain.com/blockchain/blockchain-explained/ accessed on 20/12/18

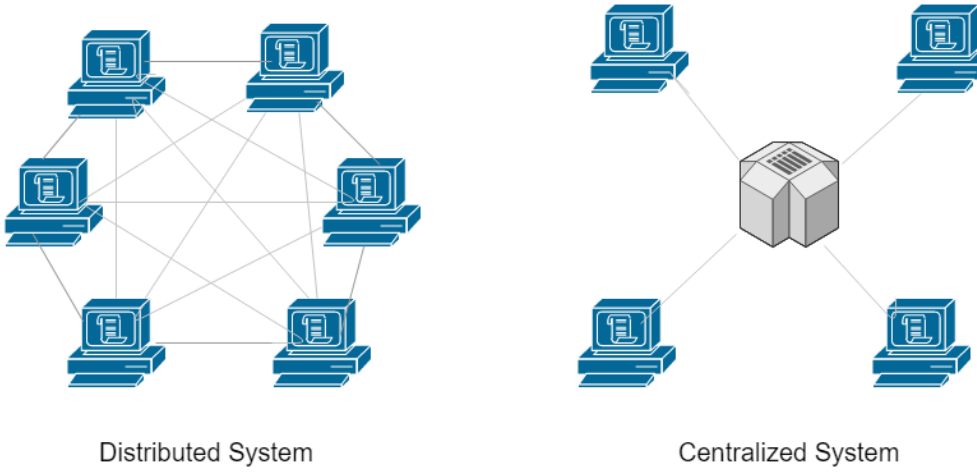

Figure 2: Distributed and Centralized system

2.5. Working of Blockchain technology

Suppose a network of different nodes connected to each other. There is no central admin in the network who stores data or holds a manageable position. Alice wants to Transfer some money to Bob. So what she does is she simply sends the money to Bob and broadcasts a message (message contain the sender and receiver info with the amount) to the network. Everyone in that network will receive that message. And by going through this each node come to know about the transaction which was done between Alice and Bob. Then each node will update that transaction information in their personal ledger which is same for everyone in that network. If another transaction happens then the same process will be carried out repeatedly, the new data is added to the ledger forming a block of chains. Here block represents a store value of the transaction.

The other benefit of not having a central database repository is that if an attacker wants to attack, it would be very difficult for him to attack all the ledgers stored at different nodes. Which is so easy in case of the single central database.

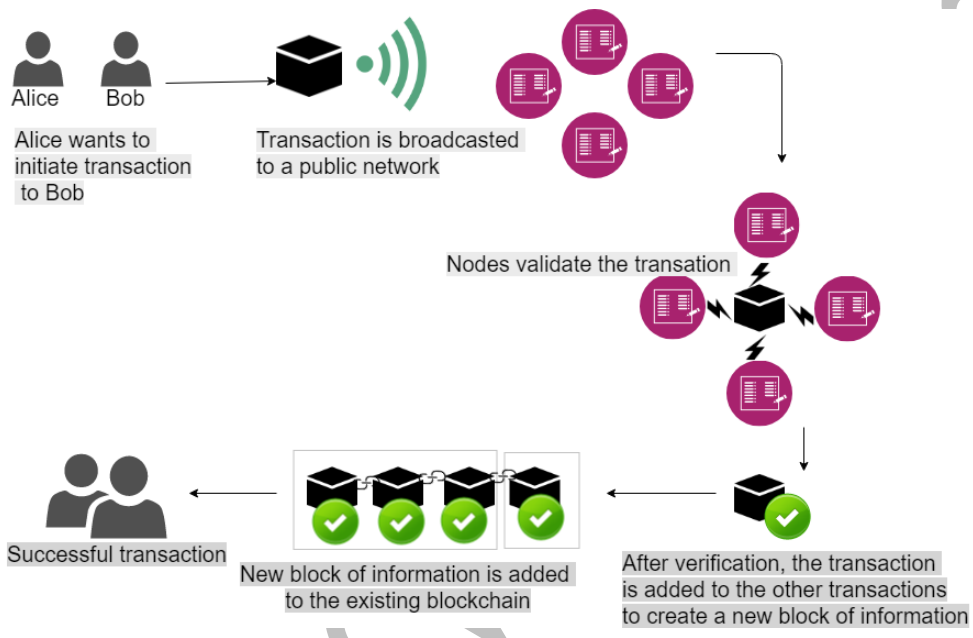

Fig.3. Blockchain process diagram

2.6. Classification of Blockchain Ledger

The taxonomy of Blockchain is based on the concept of who can access the ledger in the network. On the ground of that there are two classifications:-

2.6.1 Permissionless Blockchain

In permissionless Blockchain system, anyone can join the network without the subject of the prior verification. The main advantage of this system is anonymity and Pseudonymity can be achieved

by the actors. Since anybody can join the network so a special type of mechanism is required to verify the nodes. Examples are Bitcoin and Ethereum.

2.6.2 Permissioned Blockchain

The other type of Blockchain is permissioned Blockchain. In which each node has to take special permission from authority to becoming a verifier in the network. This system is intended to be purpose-built and used to provide extra support in the pre-existing applications. The greatest advantage of this is scalability. As all nodes need permission to be a smaller a number of participants need to operate. As the number is small so it's very easy to collaborate or alter any rule or revert transaction that is why only trusted party is allowed to act as a verifier. The example of permissioned Blockchain is Ripple, Hyperledger, and Eris.

Figure 3: Permission vs Permissionless Ledger

How nodes come to know about the authenticity of the Transaction?

Without any security features none of the systems is secure, and here we are dealing with sensitive and financial data so security becomes the most prioritized thing. As the acceptance of any system is proportional to the extent of its security.

By taking the above example, let's see another scenario when someone broadcasts the false information of a transaction which has never happened.

Alice sends 100bucks to Bob but broadcasts a message stating that she has sent 200bucks to Bob. Maybe possible that someone else has broadcasted false information about the transaction which has never happened. As all the nodes are unknown to each other so how can one show trust to another node?

In case of a centralized system, the admin or Third party was responsible for the authenticity of the person like the bank has data of you and your beneficiary whom you are going to send money. But in case of the Blockchain, How this can be possible if one does not know the other?

All this possible with the help of Digital signature and hash function. The digital signature ensures that whoever broadcast the message of the transaction is a legitimate person. In other words, digital signature checks the identity of the person. The hash function is used to check that information is correct and without any modification.

2.7. Example of Blockchain Application

As discussed earlier Blockchain technology is used for providing peer to peer connection between different systems without the involvement of the third party. So this technology can be used in parallel with the existing technology where there is a need for fast, reliable communication between different users. Also, in the applications where anonymity is required.

Some of the famous examples are- Tezos a Blockchain project that governs itself by voting of its token holders.[4] Blockchain technology can be applied to confirm user identity in the Digital

[4] Available at https://blockgeeks.com/guides/what-is-tezos/ , accessed on 20/12/2018

Identities, Passports, Decentralized notary, “Arcade city” is the decentralized global community of peer-to-peer taxi provider app.

Here are some domains where we have seen the integration of Blockchain technology in recent years:-

1. Cryptocurrencies- Cryptocurrency or virtual currency is the first application in which we came across the term "Blockchain". At the time of writing this paper, there were over 1384 cryptocurrencies available in the market.

2. Banking- Blockchain is the most talked through topic in banking sector these days. Banking services include a transfer of values across borders which is not so easy task. Blockchain speeds up the transaction process and reduces the operational cost significantly.

3. Data storage- Data is the most valuable asset for any organization as well as individuals. Currently, the single system as well as cloud-based storage both uses centralized approaches when it comes to data storage. This centralized approach can be subjected to a single point of failure like for example, as a result of a power outage or always been under the fear of cyber attack as we have witnessed so many data breaches in recent years. To overcome this problem we can use Blockchain based data storage which is distributed database across the network.

4. Smart property- Blockchain technology can be used for registration and transfer of property and valuable assets. The first time this methodology was used and tested in Sweden. Both tangible and intangible assets can be transferred over Blockchain. This methodology can be used in parallel with the intellectual property rights, wills, art and other documents, which could be stored in the immutable Blockchain.

5. Payment and settlement- The exclusive point of Blockchain is that this technology doesn't involve any third party to facilitate any transaction. In any supply chain industry, the whole process is dependent on the payment transaction between supplier and customer. Blockchain speeds up this process.

CHAPTER - 3

THE IMPORTANCE OF TRUST FACTOR

CHAPTER- 3

Key Topics Discussed in this Chapter

- Importance of Trust Factor
- Trust Through Distributed Ledger and Blockchain
- Consensus Protocol
- Challenges must be taken care of before going to Blockchain based Solution

3.1. Need For Trust

Every type of Economic exchange requires trust regardless it is initiated through the online or offline medium. At the most basic level, we should have a practical expectation that the party and institutions with whom we do trading will not take any type of advantage of us, regardless of our capacity to monitor their actions. Without this expectation, we don't feel safe during the process of transactions and the risk always fades the actual likely potential benefits of engaging in trade.

Within a limited area or we can say a small community, trust is always supported and preserved through a dense web of social relationships. However, when individuals trade with parties outside the boundaries of their reach, they must rely on other means to create confidence. This includes should be supported by a third party institution that helps in improving monitoring and enforce a contract.

Whenever we wish to send money to friends or family members, we have to rely on service to oversee the transaction. Today, almost every type of economic give-and-take that takes place outside of face-to-face cash transactions requires the involvement of a trusted third party (in fact, it can be argued that even cash transactions also oblige a reliable third party). When we purchase any things online, we depend on a credit card company or bank to verify and process the payment.

And when we want to institute an ownership claim to an asset, we rely on central authorities, including the government, to confirm our property rights.

By authorizing the identity of contributors to a transaction, supervision clearing, and clearance, and conserving the record of the exchange, these intermediaries reduce doubt and enable exchange between parties that may have no reason to trust one another. Therefore, they develop the box of potential chances for exchange and unlock potential growth.

Though, there are numerous reasons why we do not want to rely on third parties to provide these functions. First, and most understandable, are the fees that intermediaries charge for their services, which can be quite high. Always depending upon the third party can also be incompetent. This can be the case of cross border transactions which might require multiple intermediaries' third parties and usually takes 3-5 business days to complete the process. Sometimes relying on intermediaries also causes cybersecurity risks, as for example storing sensitive data on central servers creates a single point of failure.

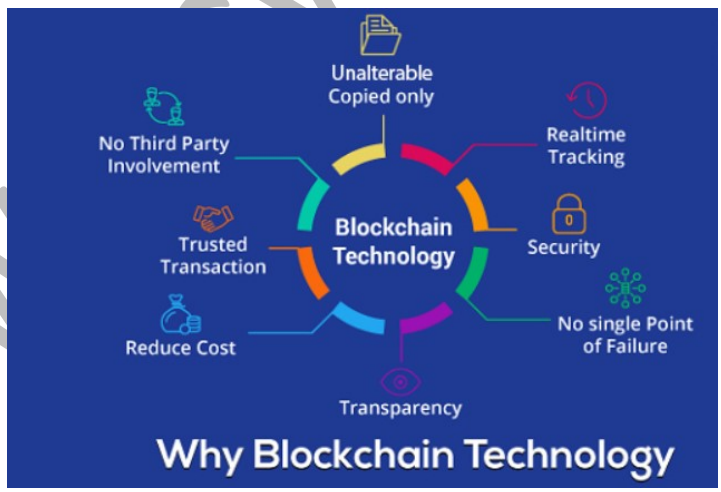

Figure 4: Blockchain Advantages

3.2. Trust through distributed leader and Blockchain technology

Traditionally we use physical record where we store all the information. A ledger is a book or system that store the records of transactions.

Now think through the way the ledger is shared. The massive majority of computing services that we use today follow centralized networks, in which a central hub or "server" stores and distributes information to other computers on the network called "clients." In contrast, Blockchain systems lane on peer-to-peer (P2P) networks in which all nodes (or computers) have equal status and simultaneously function as both client and server to one another. The main advantage of this approach is that there is no kind of the single point of failure which we have seen in the case of a centralized server.

Every node that takes part in transaction stores an up to the minute version of the ledger and participates nodes information and the consensus process.

The state of the ledger reflects the consensus reached, that's the reason Blockchain is frequently denoted to as a "single source of truth."

If the talk about the operations of a large organization, like a multinational bank, that spends significant resources in reconciling records with other counterparties, the ability of a Blockchain to update automatically and nearly simultaneously across participants (synchronization) could save a significant amount of money.

3.3. Consensus protocol

An agreement could be generated by when a node in a network works intensively in solving a cryptographic puzzle that once solved gives an output in a form of a record of transactions that all participants can see. This whole working process is considered as proof of work.

A large amount of brute computational force is required to solve the proof of work in which the computers in a network make large numbers of guesses per second to obtain the answer of that puzzle.

This requires a substantial investment in computer processors and electricity, which again makes it tremendously costly and thus enormously tough for fraudulent actors on the network to overpower honest ones. By doing so, the competition maintains the integrity of the ledger.

3.4. Data structure

Nodes continuously monitor the network for incoming transaction messages and group these transactions into blocks. The information in the blocks then serves as input into the proof of work challenge. Once a node becomes the first to solve the challenge, it “seals off” the block it is working on and sends it to other nodes on the network to verify the solution and that all the transactions in the block are legitimate. This verification happens within seconds and, once complete, the new block is added to a Blockchain.

Nodes ceaselessly monitor the network for incoming transaction messages and cluster these transactions into blocks. The knowledge within the blocks then is input into the proof of work challenge. Once a node becomes the primary to resolve the challenge, it “seals off” the block it's engaged on and sends it to different nodes on the network to verify the answer which all the transactions within the block area unit legitimate. This verification happens among seconds and, once complete, the new block is sum up to a Blockchain.

Each block added to a Blockchain contains 3 vital items of data added to a record of recent transactions: a timestamp, that establishes the approved order of transactions; associate alphanumerical string referred to as a hash, that cryptographically combines all the info in a block into one distinctive value; and a regard to the previous block’s hash. The hash provides a novel ID for every block and, significantly, reacts to even the tiniest modification within the underlying dealings information by changing in an unpredictable method.

Including a link to the previous block’s hash in every new block creates a sequence between them that extends all the method all the way down to the primary block created. The existence of this chain combined with the sensitivity of hash values to modification act as a safeguard against

tampering: if somebody were to undertake to change a transaction in a block, it might trigger a modification not solely to it block's hash however additionally within the hashes of all the blocks after appended to the chain, creating it simple for the network to discover (Lewis 2016). To hide

up any traces of tampering, an associate attacker would want to win multiple proofs of work contests to publish not solely the block containing the altered transaction however additionally all the blocks that came once it. The likelihood of having the ability to try to this decreases exponentially because the variety of blocks will increase, creating records hold on a Blockchain effectively immutable once spare time has passed. This creates the chance of exploitation the Blockchain to store valuable digital assets, together with land titles and contracts.

The method information is kept and connected on a Blockchain additionally makes it simple to trace the movement and source of assets, as well as not only cryptocurrencies however also any physical asset that's tied to a digital token.

In summary, Blockchain technology's strength stems directly from these 3 factors and therefore the approach they interact: the distributed nature of the ledger yields transparency and synchronization; the agreement protocol negates the requirement for trust; and therefore the approach information is recorded, keep and connected yields fixity and traceability.

3.5. Challenges must be taken care of before going to Block Chain based Solutions

Challenges that concerns about the issue of data privacy, operational resiliency and operational governance must be addressed prior to the wide step adoption of Blockchain based development models. There is always a need to work on this domain and educate aware of the development community about the uses and benefits of this technology including the awareness of its limitations.

Following are some major concerns which need to be taken into account.

3.5.1. Data Privacy

Ethereum Founder Vitalik Buterin has noted, *"neither companies nor individuals are particularly keen on publishing all of their information onto a public database that can be arbitrarily read without any restrictions by one's own government, foreign governments, family members, coworkers, and business competitors*" (Buterin 2016).

The main advantage of Blockchain based cryptocurrency is it provides pseudonymity for its users, like we have experienced the same in Bitcoin, but many Blockchain based solutions are required that linking of sensitive data with an individual identity like linking a property name to the owner or identifying information to an aid recipient which again raise concern about the individuals privacy.

Alternative can be using a permission network system that can help to diminish some concerns about the user's data privacy issue by but monitoring and limiting the number the actors that can take participate in the network and can access a ledger but only to a degree.

Like nowadays many financial institutes continue to research with different aspects of permission ledger system but again privacy remains to be a tough challenge to solve. Not unexpectedly, many financial institutions remain doubtful about keeping their transactional information over a distributed ledger because of their obligation requirement to protect their user's privacy and their need to keep sensitive their personal commercially trades. Now at a great pace variety of the solutions to the privacy challenge are now exploring Scientists that includes the use of "bidirectional payment channels," which enable some exchange information to be put away off a Blockchain, and the utilization of zero-learning proofs, which enable exchanges to be confirmed openly without uncovering any hidden information about the exchange However, every one of these methodologies includes tradeoffs and none has been tried in reality yet.

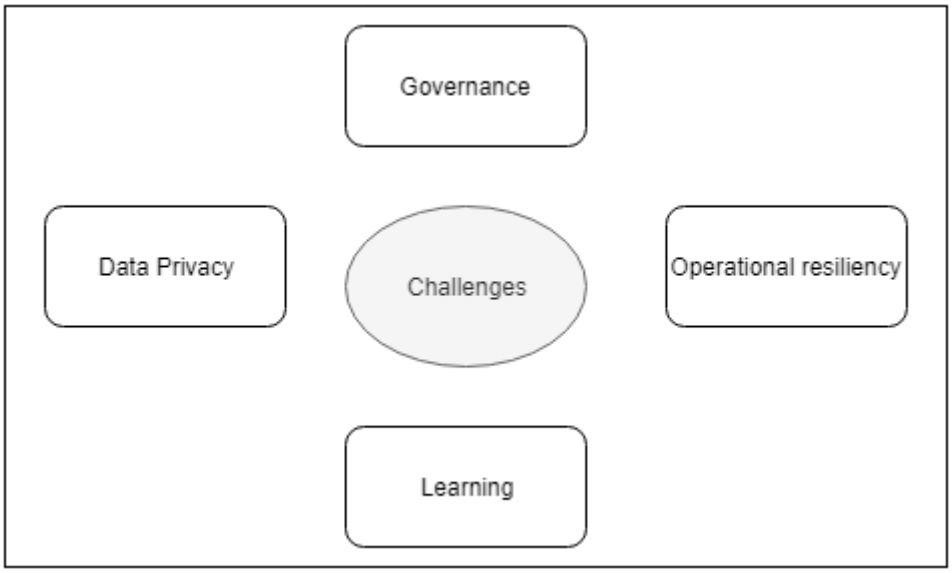

Figure 5: Blockchain challenges

3.5.2. Governance

Every organization that wishes to operate on a public Blockchain based solution should accept that it will have technically no control over the governance of the system. Must of the Blockchain technology seems stems from its decentralized operational nature, that try to replace out the role which is played by the trusted third party or intermediaries with a peer-driven consensus process.

Though, a decentralized feature also raises questions regarding governance, i.e., "who dictates and enforces the rules of the system" (Financial Times 2017).

Even though formal decision-making rule is also absent in both Bitcoin and Ethereum, in practice for the implementation of changes to existing protocols each of them has to depend on a core group of developers, which are usually made only after a degree of consensus among participants on the network has been reached.

Assumed the most of the solution related to Blockchain involve keeping valuable data on a Blockchain so it is hard to consider that the organizing like banking institute taking this risk.

In its place, they will move towards arrangements that keep running on permission systems, where they can keep up more noteworthy (though perhaps not total) control for rule design and dispute resolution. However, in the case of permission system, there is still a concern about how to best structure guidelines to address the issues of different participants and this job becomes more troublesome as the number and assortment of members permitted on the system increments.

3.5.3. Operational resiliency

The major point of attraction of Blockchain technology is that it improves the capacity to recover quickly from difficulties by moving data from a centralized structure that always be a concern of single point of failure to a distributed ledger that run on many nodes.

This advantage enhances the operational beauty of Blockchain since it helps the organization to back up their sensitive data on multiple servers, but again, the biggest problem is that Blockchain technology stays untested at large scale. Most of the solutions are proposed for use by large organizations e.g., governments, global banks, multilateral organizations, international non-profits that be likely to be risk-averse, slow to innovate and rely on those structures that are on a continual improvement phase, tried and tested again and again over many years over which numerous bugs have been successfully resolved.

Many of the solutions are intended for use by those organizations (e.g., governments, global banks, multilateral organizations, international non-profits) that tend to be risk-averse, less innovative, and depends on those systems that demands continual improvement and have been tried and tested over many years for resolving bugs which come in picture over time. Consequently, For that purpose, and because moving to Blockchain-based framework often requires wholesale rather than incremental change, they should see proof of noteworthy advantage with little risk before they think about doing a switch.

3.5.4. Learning

To overcome form the above challenges and issue, organization that is going to implement Blockchain based solution despite it is private or government organization they must train their staff. Learning not only limited to the understanding of Blockchain but also with the related

technologies, benefits and demerits of Blockchain based solution. Blockchain is like another database or record keeping system with some benefits. So end user must be skillful enough to decide what to insert in block or not. As once block is written it cannot be modified. Lots of technical knowledge is required to become master in this domain. Knowledge share between deployment companies and technology communities is required. Development organization willingly help startup in resource and knowledge sharing processes in order to expand the knowledge draw lesson from both past success and failures.

CHAPTER 4

APPLICATION OF BLOCKCHAIN TECHNOLOGY

CHAPTER- 4

Key Topics Discussed in this Chapter

- Use of Blockchain in Property Rights
- Blockchain Technology in Education System
- Blockchain based Motor Insurance Management
- Blockchain in Agricultural Industry
- Blockchain based E- Voting system
- Use of Blockchain in E-Governance
- Blockchain in Healthcare Industry
- Limitation of using Blockchain Technology

4.1. Use of Blockchain in Property Rights

India has seen tremendous growth and development in term of a standard of living. The government must look into the current economic thrust and put their efforts to capitalize this moment. They must invent this capitalization to reform its agenda. This new technological era has some power to reform the administrative departments in India. To maximize the potential benefits from technical paradigm PM Modi government started digital India mission in 2014. Since then we have witnessed the many new schemes and functional changes in the current government plan all these are done to only gain the efficient delivery of government services.

The area which required most attention is the property market. Although an initiative was taken through a Digital India Land Records Modernization Programme (DILRMP), Our Land title system still infected with some deficiencies and weakness.

There is a need for decentralized, open to access, reliable and transparent method for the record keeping in the administrative department must be needed with some legal framework. Here we see

the potential of Blockchain Technology to pride a base for a framework which can be the solution for the above problems.

For any kind of property, it is important that there is some kind of accurate record which identify the current owner with some kind of proof to preserve their ownership.

At any given point of time, these record must be able to prevent the misuse of ownership and protect owners' rights, can help in solving the dispute, prevent fraud at the time of selling and reselling the property and ensure that the ownership is transfer to a new owner after the sale of the property. For this record must be protected and only accessible to an authorized person. Unfortunately here the owner of the property has to rely on the third party for proper management of the records. Like in India government is responsible for the custody of land titles ownership and in the most of the cases these documents are not handled and managed in a systematic way.

For a clear view of the problem let's try to understand the limitations in the current system which are responsible for handling the property titles.

- Fraudulent transactions are now common case due to lack of efficiency in government operations.[5] In some cases, government acquired properties have been mortgage by people to obtain loan from a bank.
- Currently, the government is using disparate databases to store records this information handling architecture still allows ease to manipulate and alter the data.

[5] Available at https://economictimes.indiatimes.com/industry/banking/finance/banking/from-credit-risk-to-operations-risk-in-banking-lessons-from-the-diamond-heist/articleshow/63004193.cms?from=mdr, accessed on 2/12/2019

- Accountability and transparency offered by the government for centralizing record keeping system and registration system is still at a minimal level.
- Because of no systematic arrangement of operations sometimes critical data is not available when required, this results in increasing the of decision making.
- Country economic growth is likely to be dependent on infrastructural projects. But because of poor record management system cause delay in the infrastructural projects and cause inconvenient to the property buyers.

- Also, the update in the records are sometimes hard to see due to the gap between the coordination between different nodal agencies handling land records, the listed information is not standardized.
- Last but not least the current system is full of corruption. Approximately about 600 US dollar bribe exchange at the registration office. In most of the state digitized land registration database and digital land record database has not been linked together this creates problem in seamless submission and verification of documents for property registration.

These are some common and known problems in the current DILRMP system. It not results in the inefficiency and delays but also indirectly affecting Indian Economy and directly increasing the informal credit sector in India. Most of the poor and illiterate farmers in India, bound to go to informal moneylenders due to the lack of formal titles to their land.

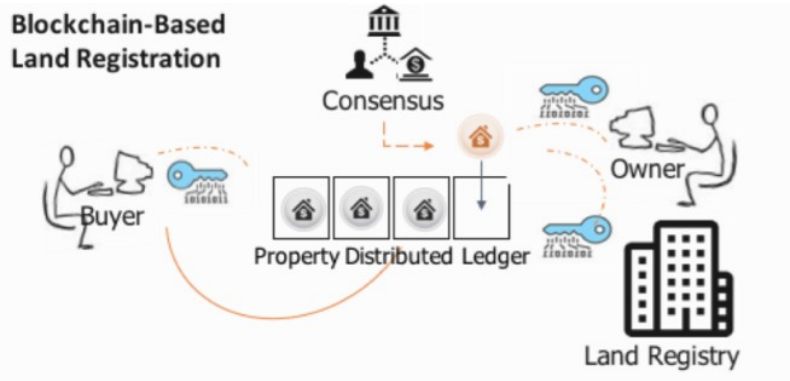

Figure 6: Blockchain based Land Registry

Solution to the problem: Smart Contract

The beauty of the Blockchain is it is based on the decentralized system so it made possible to create the record in digital form and distributed over each participant in the network in that each transaction is verified by cryptography without any involvement of the third party. Most of the problem in the current land registry and management system is, it is dependent on the trusted third party for systematic record keeping and management. For the reinforce of the current system, There is a need to eliminate the trusted third party factor from the overall land registration and management system.

Now the question is, it is possible to use a distributed system that won't rely on trust to keep the ownership information of properties?

Thing needs to understand here is how the Blockchain can be used for land registries. Blockchain can act as an instrument for ensuring accuracy. Smart contract based land title registration and management system could be one possibility. Another can be any Bitcoin Blockchain based public ledger system.[6]

[6] Available at https://coincentral.com/blockchain-land-registry/ ,accessed on 6/3/2019

These solutions are self-verified and tamper-proof, as they run on a network of different nodes so it's impossible for the owner to change the stored value in it. None of the associated parties can change the conditions written in contract so it is to assume this execute in the same way as it was initially written. Some countries like Sweden, Georgia, Ghana, Dubai, Columbia, and Netherlands started looking into it.[7]

Certain conditions and prerequisites for the adoption of Blockchain Based Property ownership recording systems are-

- This required Public Key Infrastructure (PKI) for cryptographic trust meeting. The government has to establish some criteria and provision in the current regulatory system for the successful execution of future projects.

- To maximize the output protocol like the Uniform Economic Transfer Protocol (UETP) needed that maintain the association between the buyer, seller, the payment, the banks, smart contract, and registry.
- Smart phone is the basic need for successful execution for any digital campaign. Effort must be taken to provide cheap smartphones with certain important security features. Places like India that hold poor literacy rate and around 34% of the population have access to the internet. [8]
- Although the price of mobile internet plan reduces still they are expensive for the majority of the population.
- Establishment of the National agency for monitoring and protection from the cyber threat.

[7] Available at https://www.undp.org/content/undp/en/home/blog/2018/Using-blockchain-to-make-land-registry-more-reliable-in-India.html , accessed on 6/3/2019

[8] Available at http://www.mckinsey.com/industries/high-tech/our-insights/offline-andfalling-behind-barriers-to-internet-adoption , accessed on 6/3/2019

Fact: "*There is an organization named Sankya Labs in Bangaluru that has developed a chip that uses television White Space, or wasted spectrum bandwidth, to supply internet to scores of rural households*."[9]

4.2. Blockchain Technology in Education System

The economic growth of a country is the outcome of so many factors like government policies, natural resources, fiscal status, etc. A country which is growing fast has backend support of virtuous government policies and technical advancement. All these factors directly or indirectly depend upon how a county manages its human capital?

Education adds to economic growth by providing specific skills and values. A country having good literacy rate always rise up in the graph of development. Good literacy rate also contributes to economic growth by improving health and raise the standard of living and bring political stability.

The current system of education is filled with some disadvantages. We do have many renowned educational institutions, provides a high standard of education. But the problem is seats are limited in numbers and everyone can't get into it. So they have to look for a lower rank institution. Sometimes students got trapped into it.

The skill set and knowledge provided by these type of colleges and schools are not up to the mark. Another problem is the employment issue. In India, there is a huge competition for getting a job. Attainment a good job is not easy so sometimes people tend to adopt some fraudulent activities. They try to get a job by applying through a fake certificate. In India this type of frauds are increasing day by day.[10] There is a need of proper management for certifications so the employer should be able to verify the certificates. Other concern is the lack of proper feedback system in an

[9] Murali, Anand . "Pruthvi, a chip, can connect India's rural population to the internet." The Economic Times , October 19, 2015. http://economictimes.indiatimes.com/tech/internet/pruthvi-a-chip-canconnect-indias-rural-population-to-the-internet/articleshow/ 49445899.cms

[10] Available at https://www.hindustantimes.com/education/police-gets-list-of-20-people-who-got-jobs-with-fake-edu-board-degrees/story-9LZaxFQac4Zv2XB5UqgPZL.html , accessed on 3/4/2019

educational institution. Feedback is not only required for the students so that they improve themselves on the ground of reviews. Teachers and faculties also to be reviewed on a regular cycle so that institution can confirm the faculty must be eloquent to their subject. Then only they can deliver meaningful information.

Here we must focus on, how we may use Blockchain for solving education problems?

Blockchain Technology for distributed digital records

The distinguishing feature of a Blockchain is it is single linked records of different events stored over different participant's nodes. It has some useful property like entire records is distributed over each participant so is resilient to the loss of infrastructure. Once a block containing information of records has been added by consensus among each node, it cannot be changed or removed even by the creator of that record. It is very easy to confirm the identity of any modification to the record. The events are not publically readable without a digital key but are publically accessible by anyone.

The above characteristics of Blockchain can be used of store degree certificates and record of credit and achievements. The scholastic data could be added to the Blockchain by the awarding institution. This information can be accessed by the students. Students can share this with employers or link from an online CV.

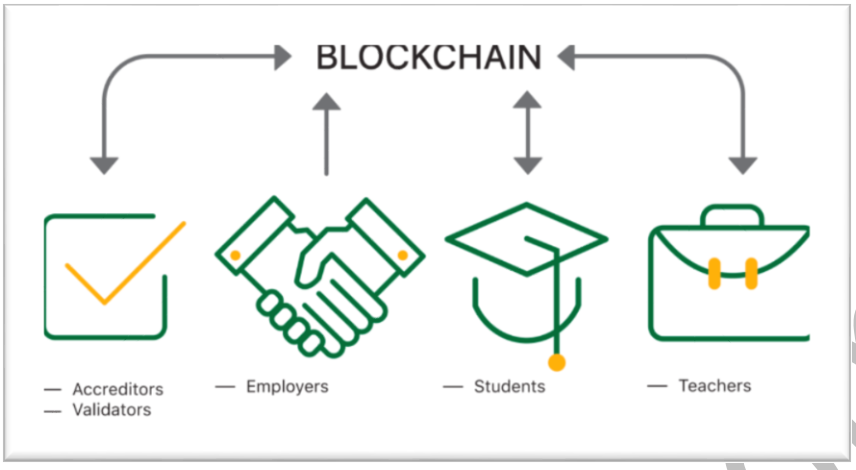

Figure 7: Blockchain in Education

Advantages

It helps in providing a persistent public record, which protects from changes to the institution or loss of its private records. This setup gives future opportunities by trusted experts and teachers for direct awarding of badges and records.

For issuing academic records whose authenticity can be verified by Blockchain is firstly used by the University of Nicosia.[11] The Blockchain gives public proof that a student is received a certificate from an authentic institution, but does not of itself. It verifies the authenticity of each party. That the reason giant company like Sony global has announced the development of Blockchain based solution for storing the educational records. [12]

[11] Available at University of Nicosia. Academic Certificates on the Blockchain. http://digital currency.unic.ac.cy/free-introductory-mooc/academic-certificates-on-the-blockchain/ , accessed on 4/4/2019

[12] Available at Sony Global Education. Sony Global Education Develops Technology Using Blockchain for Open Sharing of Academic Proficiency and Progress Records, 22 February 2016. http:// www.sony.net/SonyInfo/News/Press/201602/16-0222E/index.html ,accessed on 4/4/2019

The main benefits of adopting Blockchain based distributed record keeping system is that very first its remove the concern about the trustworthiness of the documents as it's impossible to alter the document and the record is digitally is signed by the institution so that it ensures the authenticity of the documents. Again these records can be rechecked and verified whenever it required. So the fraudulent activities can be removed especially in government sectors. So its ensure only a skill full person could get a responsible position so that the country can utilize their leadership and knowledge for the growth of the society.

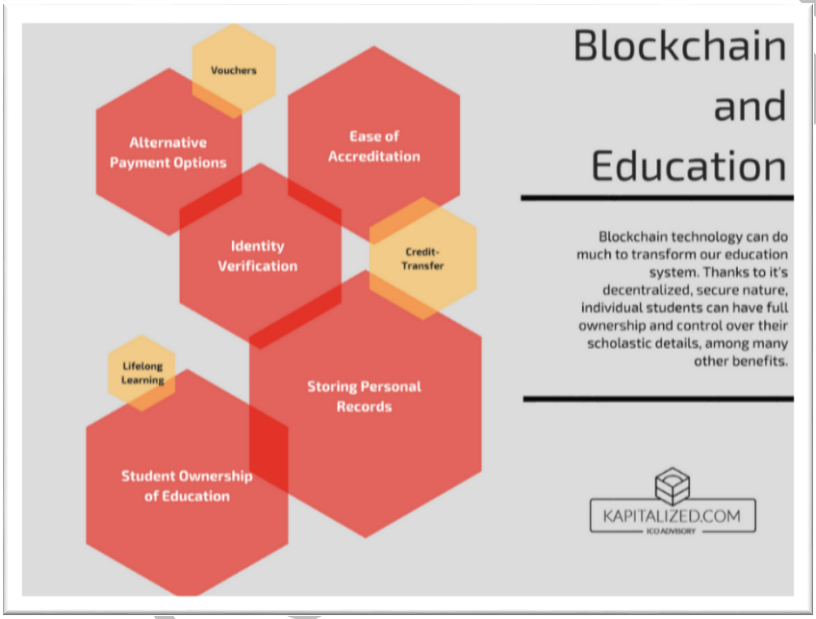

Figure 8: Advantages of Blockchain in Education source: kapitalzed.com

4.3. Blockchain-based Motor Insurance Management

In India Insurance Regulatory and Development Authority of India's (Irdai) is responsible for vehicle insurance. This agency creates and govern policies related to vehicle insurance. According to the General Insurance Council (GEC) around 60% of vehicles running on Indian roads are

uninsured.[13] Most of them are two-wheeler vehicles. The main reason behind this is that insurance is not an 'over the counter' physical product or an instant service. In our current system, processing a vehicle claim settlement is always being a problem.

Insurance companies are always being expected to settle insurance claim at the earliest when insured raise a vehicle insurance claim. However, the insurance companies have their own challenges while settling these claims. They have some predefined processes and need to coordinate with other entities like police, partner garages and are bound by certain rules and regulations.

Some usual problems which are faced by the insured,

1. No FIR

   Insured have to file an FIR at the police station in case of vehicle theft and accident. And get a copy of fir and put it with the application for the claim. Fir is not mandatory in certain cases but it helps in faster the processing and adds to the credibility of the claim.

2. No proper documentation-

   The claim settlement team find its default to process claim request which are not properly documented. claims raised by an invalid insurance policy are not settled if the expiry date has been crossed. Insurance companies sometimes need a copy of driving license vehicle registration certificate, etc. for verification. And all these will take some time for the processing which results in unnecessary delay.

3. Delayed in filing application

   It is to be advised to submit the claim application as soon as possible. It is obvious that the application might be injured or in a state of shock. However, the time for the submission

[13] Available at https://timesofindia.indiatimes.com/india/60-of-vehicles-on-indian-roads-dont-have-insurance/articleshow/56744325.cms , accessed on 4/4/2019

of application depends on the insurance company to company. It is advised to submit an application within three days to the incident.

After digitalization, the General Insurance companies are changing their operations. Their processes are now more transparent and hassle-free. However, there are some loopholes in the workflow. To understand it we have to look over the workflow of the Insurance claim process.

There are following entities who involves in the insurance process. They are the driver or vehicle owner, police, vehicle repairer, insurance adjuster, the insurance company, payment facilitator, etc. Now for understanding let us take an example of Alice whose vehicle met with an incident. Luckily Alice took insurance from the insurer. Now Alice has to apply for claim for that she has to register the incident of an accident. Traditionally Alice has to police station and file a complaint. Police will register fir and proceed for further verification. The vehicle will go for damage repair. Repair person repairs the vehicle and shares the details of the actual damage to the insurance adjuster. Insurance adjuster looks over it and negotiates and further share the details to the insurance company. Alice whose vehicle cover under the insurance have all the documents and copy of FIR then contact the insurance company and ask for an accident insurance claim. After that insurance company check all the details of the insurance policy and the feedback provided by the adjuster. If everything goes well the company will initiate the payment process and directly pay to the repair person.

Figure 9 Blockchain advantages to insurance industry

In the given system we may observe there are multiple process locks like insurance adjuster, repair person, payment facilitator, police, Alice and insurance company. They have to be synchronized in term of information so regular communication is required which takes some time. Again each process requires some time duration and after the completion of one process, the further process can only be initiated. This will increase the overall time period for the insurance claiming process. Also, chances are if there is any kind of miscommunication between entities in terms of information sharing may result in unnecessary delay or block the overall process. Although the involvement of so many middle people may result in fraud or misrepresentation.

Blockchain based decentralized web based solution

In the case of Blockchain based decentralized application, we have the following advantages –

1. Every node in the given environment has real-time updates and transactional information as they are connected with each other entity that is involved in the process like Vehicle owner, the insurance company, police, repair person, etc. have real-time information. As they are connected in hyper ledger based Blockchain network which executes them automatically like a smart contract.

2. Blockchain stands on the consensus algorithm. Therefore every transaction in the network is verified and transparency could not be compromised as any kind of misrepresentation cannot be updated into the Blockchain without undergoing thorough verification by other entities.
3. Blockchain network cannot be manipulated and every process in the system is real-time based so there is no or very minimum delay in the operations.

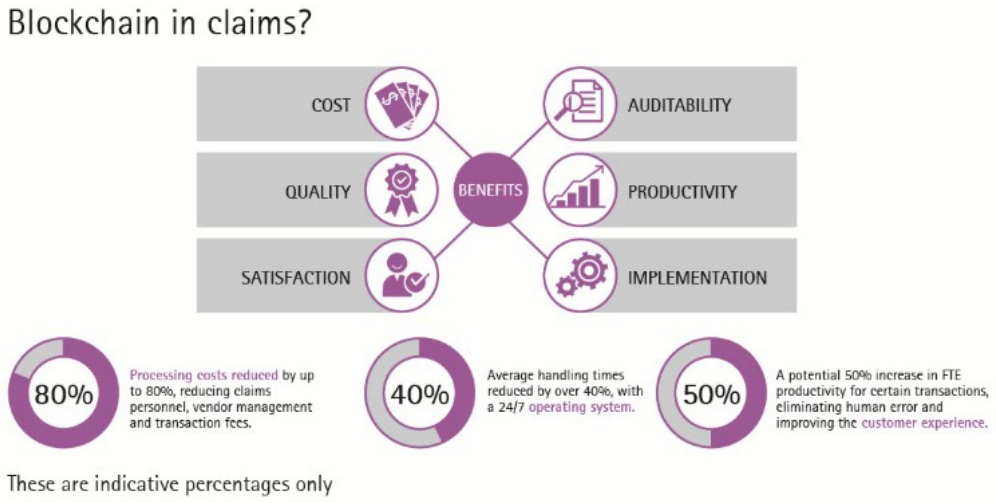

Figure 10: Blockchain based insurnce claim benifits

In this solution, after meeting with an accident Alice register FIR which will be automatically updated in the network. Vehicle repair person repairs the vehicle and updates the real-time information which will be available to every node like an insurance company, Alice, adjuster, etc.

Now Alice request the claim through the Blockchain based solution provided his insurance id. Now since every concerned person have information like FIR, vehicle repair person report, insurance details, etc. Company will validate the information and initiate further request without

any delay in the process. Based on the above information payment settlement process i.e. from payment facilitator money go to repair person account and then Alice claim will be settled. All this is done with the help of self-executing smart contract.

In this solution, because of self-execution delay will not be there and all the processes are transparent, efficient and fast due to the removal of deadlock possibilities.

4.4. Blockchain in Agricultural Industry

India's agricultural sector provides a livelihood to around 58% rural population. Agriculture, forestry, and fishing added total estimated value at Rs. 18.53 trillion in FY18. Our country is the second largest fruit producer in the world. 40% of the global workforce is dependent on agriculture so ultimately generating jobs worldwide. About US$ 8.57 billion Foreign Direct Investment (FDI) equity inflow has been attracted by the Indian food processing industry between April 2000 and December 2018.[14]

Despite being all these above benefits our agricultural sector is surrounded by so many problems. During convocation ceremony at Sher-e-Kashmir University of Agricultural Sciences and Technology, Jammu PM Narendra Modi threw some lights to the problems in this sector like the bad quality of seed, and medicines being supplied to farmers which results in low production and decreasing their per capita income too. Likewise, buyers have become suspicious of the nourishment they are devouring. For solving agro-based problem Blockchain technology can be utilized.

[14] Available at https://www.ibef.org/industry/agriculture-india.aspx , accessed on 4/4/2019

"*With Blockchain technology, this problem can also be controlled. Through real-time monitoring of the supply chain, the technology can bring in transparency in the agricultural trade — starting from the production process to making it available for the farmers as products can be examined at every stage*."

"*This will have a complete network comprising farmers, processing units, regulatory authorities, and consumers. Because one affiliated to this chain can keep an eye on this, therefore, the scope of corruption will also be reduced. Most importantly, this will check the mischievous acts of the middlemen and the harvest will not go wasted*," PM Modi said

Figure 11: Blockchain Technology in Agricultural Industry

Blockchain application based solution for solving agricultural problems

1. **Finding the source of the food**

   Food safety is being the number one concern for the consumers. Estimated $30-40 billion annually cost by the food fraud globally. Now consumers are more likely to know all the

information related to what they are consuming. This trend is pushing big industries to use Blockchain for ensuring food quality and traceability. With the news channel obfuscated with examples of fake marking, the prerequisite for anti-toxin free and natural sustenance has been taking off all the while.

Blockchain technology with the combination of some other technologies like RFID tags can be used to track down all the transaction even related to small portion whether it happened at warehouse, factory or farm itself can easily be monitored and effectively communicated across the supply chain. A lot of work has been already done globally. Giant companies like Walmart have already started with IBM to bring Blockchain technology in agro-based industries.

According to Manav Gupta, the Chief Technology Officer at IBM Canada:

> *"Even though the different players (in the food industry) all have a view to the network, they don't have complete information…what the Blockchain system allows us to do is to procure information between these different participants securely*."

For tracking the shipping of mangoes from Mexico Walmart with IBM launched a series of trails in 2017

Another British company Provenance, has implemented a Blockchain based solution to track down tuna fish from the Indonesian fishermen boats to the restaurant.

2. In the food supply chain for finding the profits of each entity

In the food supply chain, farmers are the backbone of this system. Even though they are not getting their respective due share this directly results in low farmer income. In most of the developing countries like India, the food supply chain are inefficient due to information asymmetry. With the help of Blockchain based management system, all the

processes get simplified due to the effective management of data across a network of farmers, distributors, brokers, retailers, regulators, and consumers gets simplified and transparent.

This will also encounter food wastage problem. All the members in the supply chain including farmers get access to all the information throughout the chain.

Therefore the entire supply chain become more independent and democratic and result in lesser food wastage.

The traditional mode of payment can result in a delay in the payment process. Blockchain-based peer to peer fund transfer system can address these inefficiencies. Smart contract based solution can also be implemented to bring automation in the process and will trigger payment automatically when certain conditions will be met down like delivery of the product.

3. **To find out the authenticity of the agri-inputs**

Farmers are unaware of the agro product they are buying from the local market. For increasing the profit seller used to sell fake products to the farmers. Even sometimes retailers have no idea about the authenticity of the product. All this also affect the big players like MNC who manufacture agri input. Because of fake product and cheap quality their reputation also affected.

Blockchain-based solutions help the farmers to track down the authenticity of the input product. Each product sold from manufacturer to end buyer can now have greater traceability. Farmer or retailer only has to scan the Blockchain bar code from their mobile phone and all the information related to the product like manufacturer and source of the product they are buying. After the origin of the food, item gets traced, examining contamination incidents could become an easy task.

4. **Scattering intensity of MNCs**

Currently, some multinational corporations are the dominating player of the agro-based industry. They are the largest buyers who set up the prices, buy from farmers as raw input for their product and advise them about what to grow in a particular season. However

small enterprises can again make their presence in agricultural filed with Blockchain technology.

This technology facilitates farmers to sell their products directly to users throughout the season. Therefore by elimination middle, man farmers get an attractive price in turn, allows them to stabilize their finances. Blockchain can help in solving challenges like distribution, governance and shareholding issue. Smart contract based distribution solution and tokenized shareholding create a direct connection between farmers and consumers can help small scale farmers to increase their efficiency and profit.

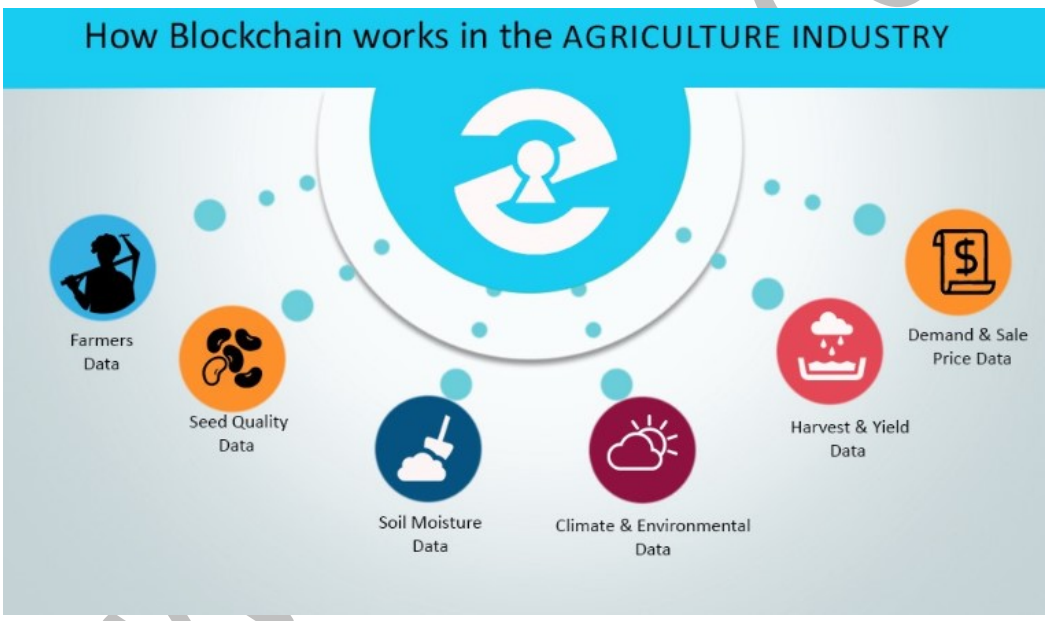

Figure 12: Blockchain application for Agricultural industry

5. Distribution of subsidies

All over the world agriculture sector is highly dependent on subsidies are given by the government. Like in India 2017-18 budget presented INR 32,000 Cr were given to farmers as a subsidy. There is always been a question about how much amount will be actually available to the farmers.

As in the formal system of distribution of subsidies many middle parties are involved so it's very difficult to trace the actual status.

However with the help of Blockchain distribution become more transparent and efficient, bringing about the successful distribution of subsidies results in pilferages the current system. Even though the actual process to establish Blockchain based network will be very difficult as multiple stakeholders have to work symmetrically, it is no longer impossible. Farmers get allocated fund in need and at the same time of need can be effectively ensured by Blockchain based effective data management.

Accountability, traceability and the quality of food can be ensured by the adaptation of Blockchain technology. In the same way with Blockchain, the food supply chain get more easily data management system across a wide network of farmers, brokers, distributors, processors, retailers, regulators, and consumers.

4.5. Blockchain Based E-voting system

A powerful democracy creates a positive image of the country. This ensures social harmony, order, and peace in the nation. A bad government always result in a bad economy. Selection of the government is done with the help of voting. Indian economy is highly dependent on the result of the election. So it is the democratic right and duty of the citizen to cast their vote and be a part of the nation making the process. However, in reality, things are not the same. According to election commission report in the year of 2014 general election, only 66.4% Indian took part in the voting process.[15] The reason behind the lack of interest might be the complicated voting procedure.

[15] Available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=105118, accessed on 3/3/2019

Also, Election requires money for setup. India is very vast county which have 29 states and 7 union territories in India. Further divided into 700 districts then 5400 Tehsils/Talukas/blocks. The total no of villages in these blocks are 600,000 villages. For carried out elections funds is required.

According to a report presented by NDTV nearly about Rs. 30,000 Crore were used by political parties on Lok Sabha election in 2014. Now the question is from where that money come?

Obviously, these are the money of taxpayers. There is a strong need for any systematic and easy operational voting mechanism. The solution can be an electronic voting system with Blockchain technology.

Estonia, Norway, and Switzerland are among those countries who initiated using E-voting system for nation wise election. For an electronic voting system, it has to be secure and capable of anonymous voting. At the same time, it safeguards from the fake voters and provides protection from tempering voters ballot. E-voting system uses public key cryptography which provides anonymity and helps in the casting of votes. Blind Signature Theorem is used to ensure that the link between voters and ballots doesn't exist.

Working of E-voting system

Initially, voter has to register himself to the appropriate authority. Then he gets his voter id with six digit pin. Then at the time of election voter has to login to the system by providing his voter id and pin then cast their vote and then gets a 12digit confirmation number. With the help of this 12digit number, the voter can check their vote by providing their voting id, pin, and 12 digit confirmation number. During the result time, the voter can also check as if their votes are taken for final counting or not.

Estonia government used an electronic voting system for their general election where the user has their voting card which is having a chip. The voter has to download a voting application have to authenticated through his voting card. Check if his name is available in the list or not. The vote is encrypted using elections public key and digitally signed by using the private key. Whenever a vote is cast it will be stored at the central server maintained by Estonia Government.

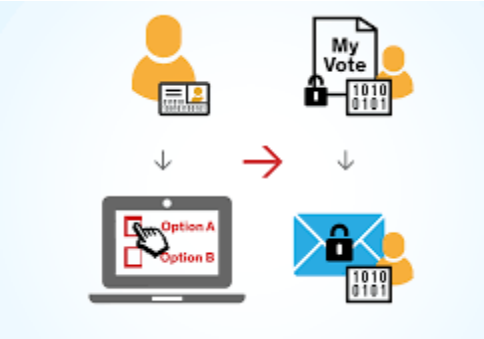

Figure 13: E-Voting system

The main drawback of this system is prone to cyber-attack. This system based on a centralized system, therefore, may prone to dos attack. The effective solution to this can be Blockchain based decentralized server which protects a user from cyber attack and maintains security and anonymity.

Blockchain-based proposed system

The first block is the special block that represents the candidate identity. Each time when candidate cast vote a note block is added to the Blockchain containing the information of the election. Unlike all transactional block first block will not be counted as it is the foundation block that contains candidates name voter identity and other information. Like traditionally voting mechanism voter can cast the blank vote. This block contains no information shows the dissatisfaction or refusal of the current political system election.

To ensure the security of the system each block is linked with the previous block so it's impossible to modify the information as it will be reflected in the system. The system is decentralized so ensure protection against dos attack and single point of failure. Each district behaves as a node where the user give his vote. His vote sends to the node and then added to the Blockchain.

Processes in the E-voting system

- User will provide his credentials like aadhar number and voter id to the e-voting system. All the credentials will be verified by the system and if matched then the user is allowed to cast his vote. This system will not allow the user to self-registration as it can cause fake identities and fill votes with illegitimate votes.
- Now voter has to decide where to cast his vote. A friendly interface will be provided to make the process simpler.
- After the user cast his vote an output is generated which contain information related to user identity, adhaar number, etc. with the hash of the previous vote. This ensures the integrity of each vote and this all information will be added on each vote cast.
- Then depending upon the selected candidate, a block is added to the corresponding Blockchain. Here each block linked with previous cast block.

4.6. Use of Blockchain in E-Governance

The beauty of the Blockchain is it provides transparency to the system. Currently, our administrative system is filled with lots of corruption. People have no knowledge about where their hard earned money is going as a tax for the development of our country. It's very hard to eliminate the root cause of the corruption in India as this was in practice since so many years. A well systematic and managed administrative system must be needed to solve these problems. That

is the reason Indian policymaker NITI Aayog decided to bring Blockchain technology in our system to enable transparency and well-defined e-governance system.

According to the report published by 6Wresearch, Indian Blockchain market will rise at a CAGR of58% during 2018-24. Many private and government sector coming together to bring out this technology. With ease provided by the government of doing businesses policies, many startups are putting their hand in this sector. Indian states like Andhra Pradesh, Maharashtra and Karnataka have started exploring the potential of Blockchain and AI technologies in e-governance applications. Although it's difficult to transform the current governance system completely it is not impossible.

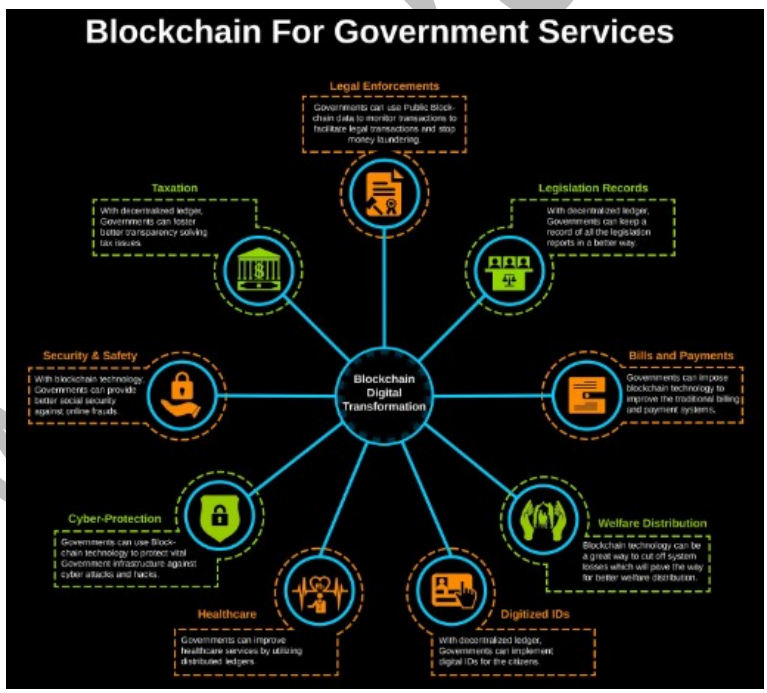

Figure 14: Blockchain for government services

4.7. Blockchain in healthcare industry

Healthcare is the basic fundamental right of each citizen. Citizen health is among one of the powerful factor that affects country's collective level of economic growth. Since development is the outcome of good health and mental peace. Unfortunately in the past health sector was poorly invested and suffered neglected.

A reported given by UNDP stated that the rank of india is 130 out of 189 countries in Human Development Index Report 2018. That portrays the importance to look over healthcare requirements in India.

Now Healthcare services in India is going through a massive change. Day by day large scale projects are getting funds from government of India. Some of them are Rashtriya Kishor Swasthya Karyakram, Pradhan Mantri Swasthya Suraksha Yojana (PMSSY) and Rashtriya Arogya Nidhi. They are some initiates taken by government to raise the level of citizen health.

It's good to see that our government started looking over it and investing in many project related to healthcare sector. One efforts is to bring digital India and E-Health together. Bringing Information and Communication Technology (ICT) in health defined E-Health. The E-Health initiatives helps in better delivery of medical services like access to medical facilities, improved quality of medical services at affordable price and very important health monitoring of Indian citizen. The aim to provide we services, mobile services and call center services that cover online consultation online medical record and exchange of patient information all over the India. Apart from government projects hospitals also store and manage patient information over their databases. However as the patient information is stored over a centralized server it also attracts cyber threats.

Another big concern in health sector is availably of fake drugs in the market. And the government is somehow unable to solve the problem of counterfeit drugs which is again a very important area to concern.

Use of Blockchain to strength the E-Health system

Figure 15: Blockchain for Health sector

- **For storing patient information**

  Medical organization usually stores patient information like Patient health information (PHI), Electronic health records, Medical insurance claims. All these information needs to be secure and collect. This is where Blockchain come in picture. As its support data integrity. Once the information is encrypted and added to the Blockchain it cannot be modified.

- **Drug Traceability**

  According to the report by World Health Organization (WHO), 35 percent of counterfeit drugs sold all over the world come from India. Fake drug selling is one of the most serious problem in healthcare industry. Selling of such drugs can be more dangerous than the actual disease as they may not work as intended and may leave patient in more severe condition. To solve the above problem we can use private Blockchain network. Drug manufacturer company store details of their products over the Blockchain. That's gives assurance of

authenticity and it is not possible to alter information once added. Therefore it is easy to detect any fraudulent activity.

Access to this Blockchain is allowed entities involved from manufacture to retailers and therefore Prof of authenticity is achieved. This process makes very easy to verify the whole communication link of the drug distribution and provide ease in tracing the drug at any given point of time.

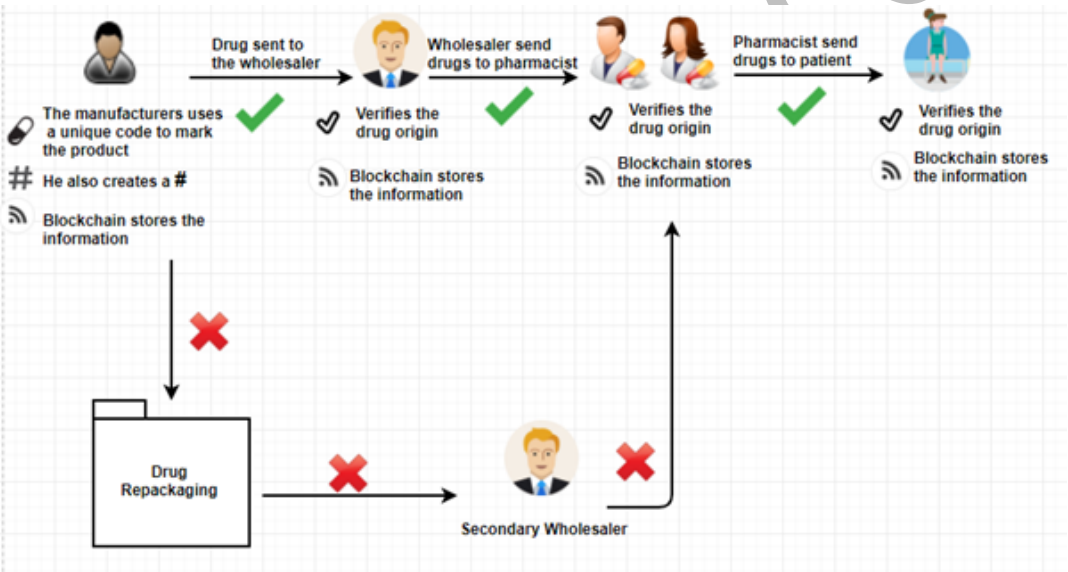

Figure 16: Drug Traceability using Blockchain based solution

- Patient Data Management

  Patient privacy comes under regulation in many countries. Although India not have any specific Law like HIPAA, that ensures the patient privacy. Another problem is that sometimes patient information have to share with third parties (e.g. with pharmacies when they need to buy specific medicines). Thus, how can we ensure the protection of data while sharing with third party at the same time?

Combines with the patient ID hash for each PHI block will be with the help of Blockchain. Covered entities can receive the required information of the patient without revealing patient's identity. In the same way, Owner of the information has full control in deciding whom to provide the access of information and up to what extent.

Globally many startups have started their operation in developing Blockchain based solution for health care industry. Some of them are Guardtime (Blockchain-based system for securing patient healthcare records), Blockchain Health (a Blockchain-based system for medical research management) and MedRec (a Blockchain-based system for securing medical records management). Blockchain is very effective technology that can help healthcare providers to prevent data breaches. It could be used as a safe and reliable method of storing and sharing sensitive data of patient.

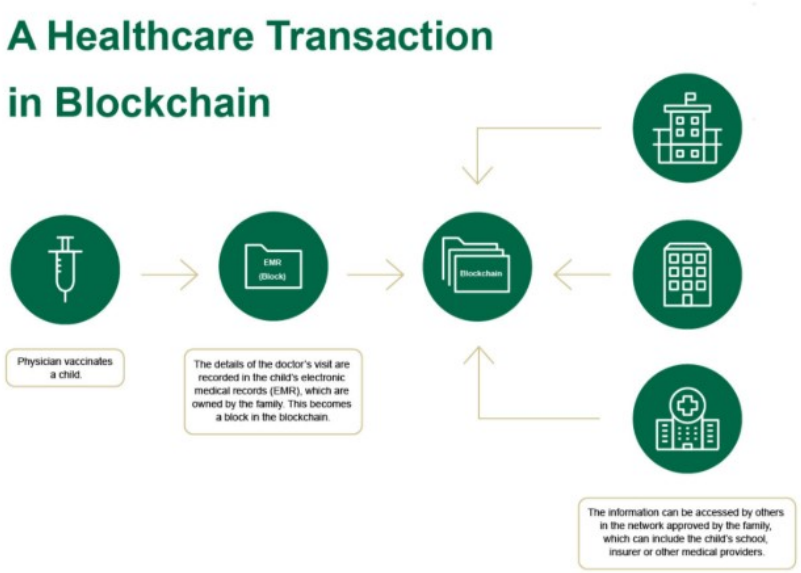

Figure 17: Patient medical record transaction process

4.8. Limitation of Using Blockchain Technology based solution

- There are number of limitation of using Blockchain based solution in India. For example in case of land title registration system, constitutional amendment and introduction to the new regulations required. Therefore lot of legislative and administrative reformation required.

- Blockchain based solution will be spine less without the support of the legislation. Reconfiguration of the current administrative regime is required.

- In case land title registration system entries within the block provide the information about the land owner. A conclusive land title law is required to handle future disputes.

- Proper infrastructural facilities are required like smart devices, mobile phone and internet. Although many low cost internet solutions are now available but still there are many regions in India where majority number of people don't have basic mobile device.

- Poor literacy rate and poverty acts as a major hurdle in the development of any digital framework.

- Blockchain based solution unquestionably cuts down the role of intermediaries. However government have to rely on partnership companies for storing initial data to the Blockchain.

- Once a data is stored over the Blockchain network it is next to impossible to modify it because modification requires each node to be updated which is very hectic task and need very powerful computational power. So value must be entered into the Blockchain with full of attention.

- Sometimes a system requires verification of an entity. As in case of decentralized system there is no central authority to govern the process and can assures the identity of an individual. Therefore practically implementation of such kind of application can become a serious problem.

- In case of educational solution, some kind of learning behavior required human intervention for reviewing of the work. Like in case of essay and presentation it's quite difficult to evaluate based on preprogrammed smart contract solution.

- Blockchain itself is very reliable and resilience against cyber attack. However there is no guarantee that the end user device is secured and protected from malicious activity. Like in case of e voting, if the user system is infected with any kind ok malicious software may result in fake or alter voting by hacker.

CHAPTER 5

CONCLUSION AND SUGGESTIONS

CHAPTER – 5

Key Topics Discussed in this Chapter

- Conclusion
- Suggestions
- Bibliography
- Glossary

5.1. Conclusion

Indian economy depends on so many factors like Agriculture, education system and current market trends. We have observed a steady growth of our economy as compared to previous years which is a good indication. However, there is still a kind of free space that can be filled. If we compare our growth with the other faster-growing countries so we may observe we are nowhere in the race of development. There is a strong urge of some reformation in the current government policies. We have witnessed an emerging technology that brings out a revolution in information sharing mechanism. Blockchain provides a reliable and secure method of sharing information with maintaining integrity and anonymity at the same time.

Blockchain technology can be used in different fields. The acceptance of this technology depends upon the trust that can be built between its users which is difficult as there is no centralized system. Bitcoin and other cryptocurrencies always are the topic of discussions. Acceptance of cryptocurrency by government bodies is needed in order to ensure the ethical use of it. Other than cryptocurrencies, we have seen the use of this in the voting system, agriculture, education and many more.

The main advantage of Blockchain technology is that it is based on a distributed system scheme. The decentralized approach helps to avoid a single point of failure. We have seen many cyber

attacks in the last few years and this graph is increasing steadily. We need upgraded technology which can be used as an alternative to ongoing technology with some added features to adapt the technology changes and enhance the security mechanism. At the same time doesn't affect the economic needs. Blockchain is the technology of different possibilities.

5.2. Suggestion

The researcher has pointed out certain suggestions on the basis of the study-

- Many factors collectively decides rise and fall of country's economic state. We cannot develop and research only for a particular domain. So we must ensure that at the ground level all the factors supporting economy cycle must be transformed as per current information driven requirement so they work more efficiently.
- Although Blockchain is the very powerful solution for peer to peer and decentralized system. But solely it is ineffective in solving the problem that infected our administrative system. So different technologies must be combined together to gain high output. For example Blockchain technology can be combined with AI for robotics distribution of fertilizers in crop.
- Implementation of Blockchain in our current system requires changes in most of the government policies which is not feasible so government first run a pilot project and based on the objective achieved they must include changes in the policies as once change it is difficult to bring changes back.
- Blockchain is a new technology, India never experienced it in past for government projects so proper benefits must be explains to policy makers and proper training and awareness program must be run to make researcher and people think Blockchain beyond the concept of cryptocurrencies.
- Lastly a technology alone cannot transform our society into a better place it's only facilitate the operation and increase the efficiency. Which ultimately result in higher throughput with some security and transparency features. So we the people who contributes to the nation.

Corruption cannot only be removed with the help of Blockchain there are many loopholes in this technology. It's our duty to support our government initiatives and give as much as we can to the society.

5.3. References

Books & E-Books:

1. Alan T. Norman -"Blockchain Technology Explained: The Ultimate Beginner's Guide About Blockchain Wallet, Mining, Bitcoin, Ethereum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA and Smart Contracts"
2. Vikram Dhillon, David Metcalf & Max Hooper "Blockchain Enabled Applications Understand the Blockchain Ecosystem and How to Make it Work for You"

Research paper:

1. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," p. 9.
2. M. Conti, S. K. E, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," *ArXiv170600916 Cs*, Jun. 2017.
3. "The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies » The Journal of Peer Production." .
4. M. Möser, "Anonymity of Bitcoin Transactions," p. 10.
5. D. Tapscott and A. Tapscott, *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. 2016.
6. "Arcade City: Ethereum's Big Test Drive to Kill Uber," *Cointelegraph*. [Online]. Available: https://cointelegraph.com/news/arcade-city-ethereums-big-test-drive-to-kill-uber. [Accessed: 24-Mar-2018].
7. "Digitisation of land records: How the relaunched programme will help overcome property crimes and frauds - Firstpost." [Online]. Available: https://www.firstpost.com/business/digitisation-of-land-records-how-the-relaunched-programme-will-help-overcome-property-crimes-and-frauds-2708226.html. [Accessed: 12-Apr-2019].
8. A. Mizrahi, "A blockchain-based property ownership recording system," p. 9.

9. D. Hamilton, "Blockchain Land Registry: The New Kid on the Block," *CoinCentral*, 11-Jan-2019. [Online]. Available: https://coincentral.com/blockchain-land-registry/. [Accessed: 12-Apr-2019].

10. Michael Pisa and Matt Juden – "Blockchain and Economic Development: Hype vs. Reality"- Center for Global Development

11. Christian Catalini- "HOW BLOCKCHAIN TECHNOLOGY WILL IMPACT THE DIGITAL ECONOMY"- MIT IDE RESEARCH BRIEF, VOL. 2017.5

12. Joseph Abadi and Markus Brunnermeier – "Blockchain Economics"

13. Purvee Pareek Gaur- "Blockchain the road ahead with context to Indian Economy"- ISSN: 2455-9040 , National Journal of Multidisciplinary Research and Development, Volume 3; Issue 1; January 2018; Page No. 536-539

14. Nicola Dimitri- "The Blockchain Technology: Some Theory and Applications"- The Maastricht School of Management

15. Supriya Thakur Aras- "Blockchain and Its Applications – A Detailed Survey"- ISBN:0975 – 8887, International Journal of Computer Applications, Volume 180 – No.3, December 2017

Web Resources:

1. Hunink, Y. (2017, March 28). Can Blockchain help reduce Energy Poverty in Rural India? (1/3). Retrieved December 5, 2018, from https://medium.com/energy-bazaar/can-blockchain-help-reduce-energy-poverty-in-rural-india-1-3-c861788c1b88
2. Emerging Opportunities for Blockchain in Development. (2018, January 18). Retrieved January 20, 2019, from http://www.fao.org/e-agriculture/news/emerging-opportunities-blockchain-development
3. Bindra, J. (2018, March 30). Transforming India through blockchain. Retrieved February 3, 2019, from https://www.livemint.com/Technology/UZIex6fPPyAqVuTHqpzZiN/Transforming-India-through-blockchain.html
4. Malte Möser, Rainer Böhme and Dominic Breuker"An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem" Retrieved February 15, 2019, from available http://maltemoeser.de/paper/money-laundering.pdf
5. Valenzuela, J. (2019, February 14). Arcade City: Ethereum's Big Test Drive to Kill Uber. Retrieved February 5, 2019, from https://cointelegraph.com/news/arcade-city-ethereums-big-test-drive-to-kill-uber

Web links:

1. https://yourstory.com/2018/08/blockchain-benefits-farmers-agriculture/
2. https://www.expresscomputer.in/news/budget-2018-govt-to-consider-use-of-blockchain-set-up-5-lakh-wi-fi-hotspots-in-rural-areas/23638/
3. https://ruralhealthit.com/blog/2018/3/4/new-grants-to-help-healthcare-interoperability-via-blockchain
4. https://www.ccgrouppr.com/practical-applications-of-blockchain-technology/sectors/agriculture/
5. https://www.livemint.com/Technology/UZIex6fPPyAqVuTHqpzZiN/Transforming-India-through-blockchain.html
6. https://economictimes.indiatimes.com/tech/internet/blockchain-can-add-5-bn-to-indian-economy-in-5-years-nasscom-official/articleshow/65163075.cms
7. https://cointelegraph.com/explained/how-blockchain-can-be-the-backbone-of-indias-economy-explained
8. https://blockchainmagazine.net/blockchain-transform-indian-government-service-critical-analysis/
9. https://medium.com/swlh/how-blockchain-technology-can-transform-the-healthcare-sector-604d1bcdc16b
10. https://ehealth.eletsonline.com/2017/07/how-blockchain-technology-can-be-the-next-big-thing-in-indian-healthcare/
11. http://www.forbesindia.com/blog/technology/how-blockchain-can-help-fight-counterfeit-drugs-in-india/
12. https://health.economictimes.indiatimes.com/news/health-it/is-blockchain-in-indian-healthcare-worth-the-challenges/64095898
13. https://economictimes.indiatimes.com/industry/healthcare/biotech/healthcare/indian-healthcare-market-to-hit-372-bn-by-2022/articleshow/61903998.cms