PUBLISHED BY
bookboon

Manmohan Joshi

Blockchain Basics

MANMOHAN JOSHI

BLOCKCHAIN BASICS

Blockchain Basics
1st edition

ISBN 978-87-403-3507-1

CONTENTS

ABOUT THE AUTHOR

Dr. Manmohan Joshi, M.A., M.Ed., Cert. Educational Admin, Dip. HRD, Dip. Mgmt. (UK), MBA, Ph.D. (Mgmt.), has over 45 years' teaching, training and administrative experience. He has worked as Principal of large and reputed educational institutions in India, Kuwait and the Sultanate of Oman.

For his work on Innovative Practices in Value Education he was awarded by the National Council of Educational Research and Training, India.

He is also the recipient of the Best Teacher Award from the Govt. of Tamilnadu as well as the Central Board of Secondary Education, India.

He has presented papers at various national and international conferences under the auspices of UNESCO. He has also conducted various workshops for teachers, students, parents and administrators. The topics covered a wide area viz., Leadership and Team Building, Value Education, Administration Skills, Career Choice, Effective Decision Making in Administration, Effective Communication Skills, Interpersonal Relationships, Continuous Comprehensive Evaluation, Skills in Dealing with Managers, Secretarial Skills. He has also authored several books on different subjects.

Later he worked as Acting Chief Executive for a reputed Training Institute in the Sultanate of Oman.

His recent formal official assignment was at a group of educational institutes in Bangalore, India, where he conducted workshops and training programmes – especially training in Soft Skills and Business Communication – for college professors and students, and taught students of MBA, B.Ed. and Law.

Currently he is a freelancer and conducts workshops and training programmes for college students, professors as well as those working in the corporate sector – particularly in the area of Soft Skills, Business Communication, Pedagogy of Teaching, Guidance and Counselling at College/School level.

He spends a great deal of time in writing books which are published as eBooks on www.bookboon.com

He can be contacted through e-mail: manmohan.joshi@gmail.com

PREFACE

We have seen that whenever any new technology is brought out, there is not only scepticism but also opposition, and blockchain is no exception! It is a fact that blockchain is happening now and is bound to increase its presence in various spheres of life. Blockchain has a disruptive potential and is already doing so in all sectors across the value chain.

Blockchain is a new way to think about cross-organisational data management, especially when we need to guarantee privacy and transactional confidentiality. The technology makes it near impossible to modify the data, and that enables trust within the network of organisations involved.

Blockchain technology brings a wide range of value propositions for businesses. In fact, no sector should ignore it because it has the potential to ease various constraints currently existing in different business operations.

It is believed that a decade from now, it is more likely than not that the blockchain will be embedded in our daily lives in ways that we cannot even imagine today. The various companies and governments have already spent billions of dollars in blockchain technology. Fortune 500 companies are investing billions in the blockchain. Businesses are using the distributed ledger technology behind Bitcoin to track their supply more efficiently.

This book has made an attempt to describe the basics of blockchain, and is likely to be of great use to management and technical personnel – practising as well as aspiring – at various levels.

I'd like to express my gratitude to Karin Hamilton Jacobsen and Sophie Tergeist for encouraging me at all stages.

I'd also like to thank the entire team of bookboon.com for publishing several of my books, including this one.

Manmohan Joshi

1 CONCEPT OF BLOCKCHAIN

1.1 INTRODUCTION

We have seen that whenever any new technology is brought out, there is not only scepticism but also opposition, and blockchain is no exception! It is a fact that blockchain is happening now and is bound to increase its presence in various spheres of life. Blockchain has a disruptive potential and is already doing so in all sectors across the value chain.

Blockchain is an ingenious invention. It is the brainchild of a person or a group of people known by the pseudonym, Satoshi Nakamoto. But since then, it has evolved into something larger.

1.1.1 ORIGIN

Blockchain technology was introduced by Bitcoin. Financial institutions showed interest in blockchain after seeing the success of a certain digital currency, and blockchain's first application was Bitcoin in 2009. Later other digital currencies appeared such as Ether. This first application aimed to provide a new way of connecting users through the use of a certain digital currency. So, what is this blockchain?

1.2 WHAT IS BLOCKCHAIN?

To put in simple terms, blockchain is a series of records of data that is managed by a cluster of computers. These clusters of computers are not owned by any single entity. We can say that it is like an open ledger that is used to record online financial transactions in chains. Each chain is made up of individual units called blocks. Each block consists of a unique code called 'hash'. Every hash also contains the hash of the previous block in the chain. They link with each other in a specific form, to form a blockchain.

We can say that it is a simple way of passing information from A to B in a fully automated and secure manner. One party to a transaction initiates the process by creating a block. This block is verified by thousands – may be more – computers. The verified block is added to a chain which is stored across the net.

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

We can further elaborate that blockchain is a record-keeping and contract-enforcement technology. It allows organisations to streamline shared workstreams – such as supply chains – by exchanging and tracking assets and transactions on a shared ledger.

Blockchain technology proposes a new paradigm capable of infiltrating, interconnecting, and in many ways, optimizing every existing system of organisation. The advantages are counted for dozens; on the other hand, the drawbacks are very few in comparison, and most of them are tied to technological, regulative or scalability issues that will be torn down with the mere passage of time.

We can further define it as follows:

- It is a ledger that records transactions without the need for a central authority.
- It is essentially a new paradigm of organisation that allows users to record transactions in a distributed shared ledger without the need of a middle-man.

Since blockchain networks are distributed among all the partners' computers, each partner has real-time visibility into every transaction.

In addition to supply chain and shared workstream applications, developers are driving new revenue streams by creating blockchain-based products and services.

So, what is blockchain technology?

A 'block' is a cluster of data within the blockchain that has a unique identifier and a history. Blocks store transaction information such as date, time or dollar amounts, as well as the digital signatures of transaction participants.

To simplify, we can say that a blockchain is a chain of blocks which contain information. Each block records all of the recent transactions, and once completed goes into the blockchain as a permanent database, and a new block is generated.

Fig. 1/1 below shows this.

Fig. 1/1 Blockchain

1.3 HOW DOES BLOCKCHAIN WORK?

Blockchain technology offers a storage system that is more resilient to database attacks than any other technology. Here the transactions are made through unique 'keys' assigned to every user in the chain. These are conveyed over the network for verification and validation for 'mining' (process of recording transaction records). The records of verified transactions are then transferred and stored in a single block.

Let us take the example of a spreadsheet which is duplicated thousands of times across a network of computers. Now imagine that this network is designed to regularly update this spreadsheet and you have a basic understanding of the blockchain.

Information held on a blockchain exists as a shared database which is continually reconciled. This database is not stored in any single location. It means that the records it keeps are truly public and verifiable. Hosted by millions of computers simultaneously, its data is accessible to anyone on the Internet.

To understand the analogy with spreadsheet, let us consider what William Mougayar (2016), blockchain specialist, has stated:

> *"The traditional way of sharing documents with collaboration is to send a Microsoft Word document to another recipient and ask them to make revisions to it. The problem with that scenario is that you need to wait until receiving a return copy before you can see or make other changes because you are locked out of editing it until the other person is done with it. That's how databases work today. Two owners cannot be messing with the same record at once. That's how banks maintain money balances and transfers; they briefly lock access (or decrease the balance) while they make a transfer, then update the other side, then re-open (or update again). With Google Docs (or Google Sheets), both parties have access to the same document at the same time, and the*

> *single version of that document is always visible to both of them. It is like a shared ledger, but it is a shared document. The distributed part comes into play when sharing involves a number of people. Imagine the number of legal documents that should be used that way. Instead of passing them to each other, losing track of versions, and not being in sync with the other version, why can't all business documents become shared instead of transferred back and forth? So many types of legal contract would be ideal for that kind of workflow. You do not need a blockchain to share documents, but the shared documents analogy is a powerful one".*

As a matter of fact, blockchain technology has gone far beyond its association with cryptocurrency and is finding relevance in a variety of fields including banking, healthcare and logistics.

It is also important to note that Artificial Intelligence (AI) and blockchain intersect in many ways. AI can pull in structured and unstructured data, make sense of them, provide insights and make predictions. Earlier we could do this within an organisation. But with blockchain, we are able to drive insights across cross-organisation business processes.

Blockchain is a new way to think about cross-organisational data management, especially when we need to guarantee privacy and transactional confidentiality. The technology makes it near impossible to modify the data, and that enables trust within the network of organisations involved.

2 TYPES AND FEATURES OF BLOCKCHAIN

2.1 TYPES OF BLOCKCHAIN

There are three main types of blockchain:

- **Public Blockchain:**
  - It is completely decentralised;
  - There is no single authority on the network;
  - All transactions on the chain are visible to any node on the network.

- **Private Blockchain:**
  - It is the property of an individual;
  - Nodes require permission to access the network.

- **Consortium Blockchain:**
  - It is a private blockchain;
  - Authority is distributed;
  - Acts in the best interests of the network.

2.2 FEATURES OF BLOCKCHAIN

The key features are:

- **Digital currencies:** They have the potential of influencing banking operations on a global scale. More and more new digital currencies are being created. They aim to operate in specific applications, such as:
  - Energy trading,
  - Incentivizing certain behaviours, e.g. SolarCoin.

- **Decision-making:** Blockchain has evolved from old organisational systems. These systems used conventional methods and relied on centralised authority. But the new paradigm – blockchain – gives decision-making capacity to the users. This results in elimination of middlemen as well as transaction fees.
- **Security of the system:** Users themselves can take control over the system's security without the involvement of a centralised authority.
- **Validity of transaction:** Blockchain has figured out a way in which users themselves can decide about the validity of a transaction. This eliminates the need for huge amounts of energy to work on current algorithms.

2.3 CHARACTERISTICS OF VARIOUS TYPES

2.3.1 PUBLIC BLOCKCHAIN

In a public chain, everybody can:

- Download a copy of the blockchain;
- Write transactions in the network;
- Participate in the consensus.

Moreover, all the users have the same rights, e.g. Bitcoin.

2.3.2 PRIVATE BLOCKCHAIN

When some restrictions are applied to certain users, we call that a private blockchain. The results of such restrictions are:

- It is controlled by a single entity;
- It can affect the reading access, the writing access or both;
- Only a central authority can take part in the validation process of transactions;
- The company operates the necessary servers, decides who gets access and is responsible for achieving the consensus;
- Blockchains consume huge amounts of energy, and the current supported number of transactions per second might not be enough for all purposes. Private chains come as a situational solution to these problems.
- Companies can use private blockchains to run pilot tests and gain experience before executing a major migration of their activities to a public blockchain.

2.3.3 CONSORTIUM BLOCKCHAIN

Consortium chains work in the following way:

- Though they also apply restrictions to some of their users, their governance is split between two or more entities.
- Consortium chains can be closer to a public or a private chain, but they have some common characteristics:
  - The consensus process is controlled by a set of pre-determined nodes;
  - The set of rules for matching and clearing do not depend anymore on the broker. They are coded in the form of smart contracts. *(Explained later in 3.5)*

2.4 PILLARS OF BLOCKCHAIN

The three main pillars of blockchain technology are:

- Decentralisation,
- Transparency, and
- Immutability.

2.4.1 DECENTRALISATION

Before we try to understand the advantages of decentralisation system, let us look at the way we have been making use of centralised services.

The basic features of centralised services are:

- A centralised entity stores all the data;
- One has to interact solely with this entity to get whatever they want;
- The most common example is that of banks. They store all the customers' money and the only way they can pay someone is by going through the bank.
- When one enters a query in an Internet search engine, they send the query to the server which then gets back at them with the required information.

Fig. 2/1 below shows this client-server model.

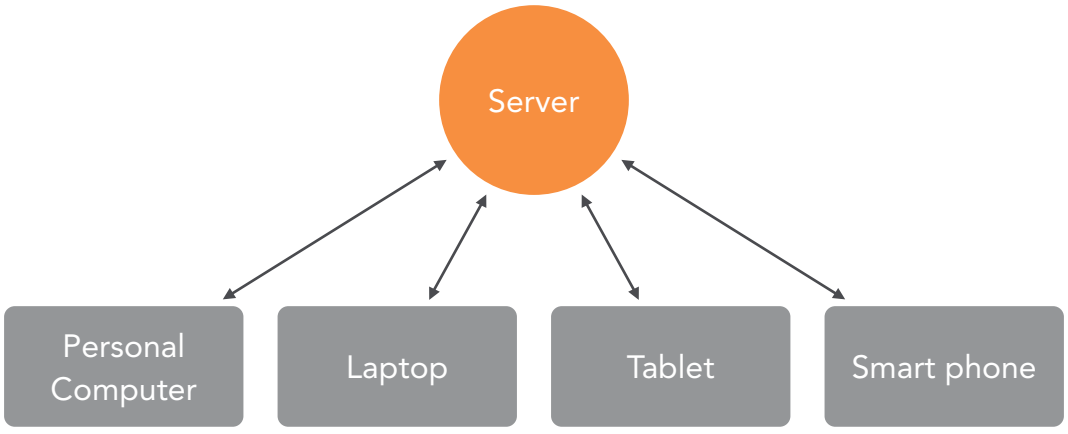

Fig. 2/1 Client-server model

Even though centralised systems have been treating us well, they have some vulnerabilities:

- There is a core authority that dictates to other entities in the network;
- Only privileged users can access the history of transactions or confirm new transactions;

- Since all the data is stored in one spot, it makes easy target for potential hijackers;
- Whenever the software is to be updated/upgraded, it halts the entire system;
- If the centralised entity shuts down the system for any reason, nobody will be able to access any information;
- If the entity gets corrupted, all the data inside the blockchain will be compromised.

Now let us look at the advantages of a decentralised system. They are:

- There is no core authority to dictate terms;
- The information is not stored by one single entity. Everyone in the network owns the information.
- One can interact with their friend directly without the involvement of a third party.
- This is the main ideology behind Bitcoins *(explained later in 4.2)*. One can transfer money to anyone without having to go through a bank
- Every entity in the network can access the history of transactions or confirm new transactions.

Fig. 2/2 below shows a comparative graph of centralised versus decentralised system.

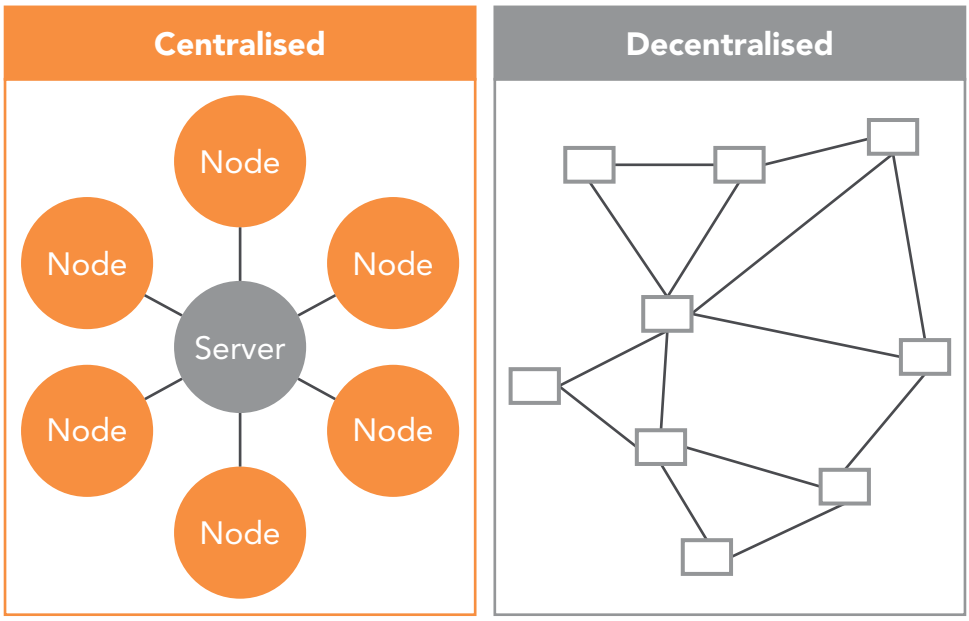

Fig. 2/2 Centralised versus Decentralised system

2.4.2 TRANSPARENCY

While it is said that blockchain gives privacy, it is also claimed that it ensures transparency. The idea of transparency works in this way:

- A person's true identity is hidden via cryptography and is represented by their public address. For example, if one wants to look up a person's transaction history, they will not see "Jane transferred 10 BTC". What will be seen will be something like this: "1BS1mnoSKrNxxx7ipSW by Mv6ZJL transferred 10 BTC". It will mean: "_____" *(name hidden)* transferred 10 Bitcoins.
- So, even though the real identity of the person is hidden – and thus secure – another person's transaction can be viewed.
- This type of transparency adds an extra level of accountability within a financial system.
- This transparency forces – to a large extent – the various entities in the network to be honest in their transactions. This is particularly relevant from the point of view of cryptocurrency.
- Because of this type of transparency, it is also possible that if the blockchain was integrated in the supply chain it will have enormous benefit for the businesses.

2.4.3 IMMUTABILITY

The concept of immutability ensures that once something has been entered into the blockchain, it cannot be tempered with. This is important for the following reasons:

- It is very valuable for financial institutions.
- It may not be possible for anyone to fiddle around with company accounts, and so a lot of embezzlement cases can be nipped in the bud. This is achieved by doing the following:
  - This happens because blockchain uses the cryptographic hash function.
  - In the context of cryptocurrencies like Bitcoin, the transactions are taken as input and run through a hashing algorithm which gives an output of a fixed length.
  - The blockchain is a linked list. It contains data and a hash pointer.
  - The hash pointer points to its previous block, thus creating a chain.
  - So, one small tweak makes blockchains extremely reliable.

Here is an example:

- A hacker attacks block 5.
- They try to change the data.
- A slight change in data will change the hash.
- Any slight change made in block 5 will change the hash stored in block 4.
- This will change the data and the hash of block 4.
- This will result in changes in block 3 and so on.
- This will completely change the chain, which is impossible.
- This is how blockchain achieves immutability.

2.5 NETWORK AND NODES

The blockchain works on the principle of peer-to-peer network. This network is a collection of individual computers – called nodes – which are interconnected with each other. These nodes – or individual computers – take in input, process the information, perform the required function, and give out an output.

In this peer-to-peer network workload is partitioned between partners. These partners – or peers – are equally privileged.

This system has the following characteristics:

- There is no one central server.
- There are several decentralised peers.

- There is no central authority.
- If one of the peers goes out of the system, there are still more peers to download from.
- It is not prone to censorship.
- The main feature of this system is file sharing, also called torrenting.
- This system is quite fast.
- There is no single point of failure.
- All downloaders are also uploaders.

Fig. 2/3 below shows the system of decentralised peer-to-peer downloading

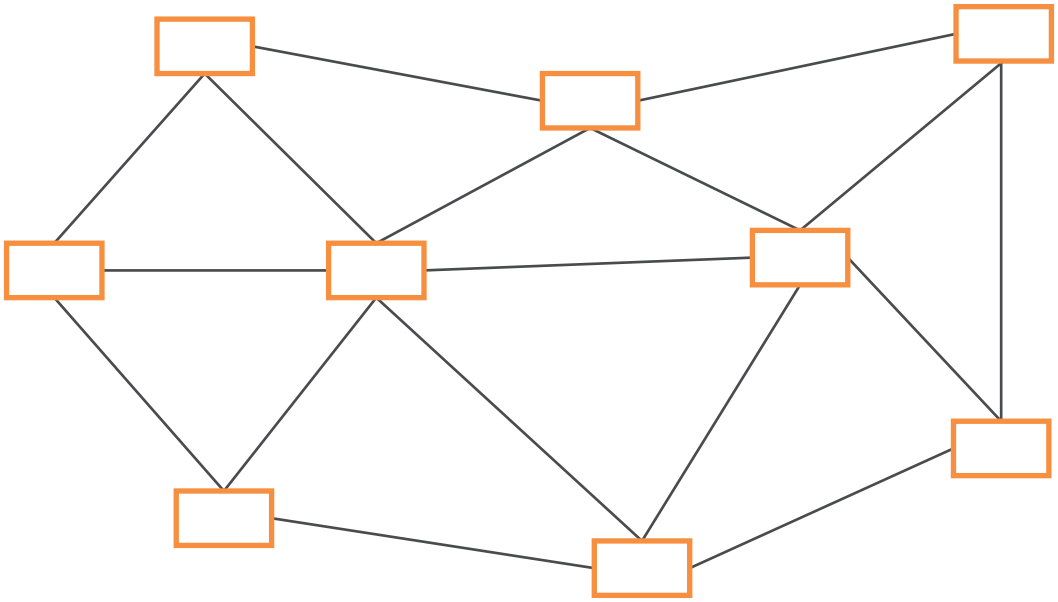

Fig. 2/3 Decentralised Peer-to-Peer Downloading

2.5.1 USE OF PEER-TO-PEER NETWORK

The use of consensus mechanism is made in peer-to-peer network structure in cryptocurrency. Cryptocurrencies use normal proof-of-work consensus mechanism. In this system all the nodes have the same privilege.

We can further say that:

- Cryptocurrencies like Bitcoin and Ethereum use a normal 'proof-of-work' consensus mechanism. *(see more in 5.4.1)*
- Ethereum will eventually move on to 'proof-of-stake'. *(see more in 5.4.1)*

- Even though the functions and degree of participation of the nodes may differ, they are not given any special privileges.
- Since there is no central server or central entity, there is no hierarchy. Thus, it is a flat topology.

2.5.2 SYSTEM OF TRANSACTION

The system works on information flow from one node to another.

This works like this:

- Suppose X sent 1 ETH to Y.
- The nodes nearest to X will get to know this.
- They will tell the nodes closest to them.
- These nodes will further tell others next to them.

Each node – computer – in the Ethereum network can do the following to participate:

- Keep a shallow-copy of the blockchain (also known as 'Light Client').
- Keep a full copy of the blockchain (also known as a 'Full Node').
- Verify the transactions (also known as 'Mining').

3 APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

3.1 INTRODUCTION

Blockchain technology has already started disrupting the financial services sector, and is gradually making inroads into other sectors.

Akash Takyar, CEO – Leeway Hertz – has stated:

> *"With the increasing demand of blockchain, everyone has started to experience the potential of this technology. Initially, blockchain brought disruption in the financial industry, but now its uses have been investigated across various industries including software development".*

It can be utilised in multiple industries including the following:

- Financial services,
- Healthcare,
- Government,
- Travel and hospitality, and
- Retail.

3.1.1 FINANCIAL SERVICES

Blockchain technology has already been implemented innovatively in financial services sector. This is done through the following:

- It simplifies the process associated with asset management and payments;
- It provides an automated trade lifecycle;
- All participants can have access to the same data about a transaction;
- The need for brokers or middlemen is eliminated;
- It ensures transparency; and
- There is effective management of transactional data.

3.1.2 HEALTHCARE

The blockchain can play a significant role in the health care sector through the following:

- It increases the privacy, security and interoperability of the data;
- It enables secure sharing of data among the entities involved;
- Overhead costs are reduced;
- There is no interference of a third-party; and
- Data can be stored securely accessible only through digital signatures.

3.1.3 GOVERNMENT

Blockchain technology can transform governmental operations in the following manner:

- It can address the data transactional challenges;
- It enables better management of data between various departments through proper linking and sharing;
- It improves transparency;
- It improves the monitoring system; and
- It provides better way for auditing the transactions.

3.1.4 TRAVEL AND HOSPITALITY

Blockchain can bring out radical changes in the travel and hospitality industry. This can be done by applying it in the following:

- Money transactions;
- Storing important documents such as passports, social security details and other identification documents;
- Travel and hotel reservations;
- Travel insurance;
- Loyalty and rewards points, etc.

3.1.5 RETAIL

Blockchain technology can be applied in the retail sector. It can be done by:

- Ensuring authenticity of high value goods;
- Preventing frauds;

- Locating stolen/lost items;
- Enabling virtual warranties;
- Managing loyalty points; and
- Streamlining supply chain operations.

3.2 BUSINESS APPLICATIONS

The blockchain network can create value and authenticate digital information. This can have several business applications. These are:

- File storage,
- Supply chain auditing,
- Know Your Customer (KYC),
- Stock trading,
- Identity management,
- Smart contracts, and
- Crowdfunding.

3.2.1 FILE STORAGE

File storage is decentralised. This ensures that the data cannot be hacked or lost. This is possible because of the use of Inter-Planetary File System (IPFS) which ensures that:

- It is conceptualised how a distributed web might operate;
- It gets rid of the centralised client-server relationships;
- It speeds up file transfer and streaming times; and
- It is an improvement on the existing content-delivery system which is currently overloaded.

3.2.2 SUPPLY CHAIN AUDITING

Ethereum Blockchain has the potential to improve the system of supply chain auditing. It is possible to do the following *(some things are already being done):*

- Ethical claims of companies about the genuineness of their products can be verified.
- Blockchain-based timestamping of a date and location can enhance transparency.
- Supply chain auditing can be performed for a wide range of consumer products.

3.2.3 KNOW YOUR CUSTOMER (KYC)

Financial institutions – and some other organisations also such as mobile service/Internet providers – perform a lengthy process to verify the identity of their customers. Using blockchain can ease this process in the following way:

- Cross-institution client verification can be done faster.
- Monitoring and analysis effectiveness can be increased.
- KYC costs could be reduced.
- Collecting scanned documents (which can be verified with issuing authority) digitally can reduce the time taken for the KYC process. Some of the applications are Polycoin, Trust in Motion (TiM).
- After verification the data can be cryptographically stored on the blockchain.

3.2.4 STOCK TRADING

Blockchain technology has a huge potential for added efficiency in stock trading. It can do the following:

- Since execution is done peer-to-peer, there can be immediate confirmations for trade.
- The intermediaries – clearing house, auditors, etc. – can be removed from the process.

Several organisations are making some use of blockchain applications for the services they offer.

Some of these are the following:

- ASX (Australian Securities Exchange)
- Deutsche Borse (Frankfurt's stock exchange)
- JPX (Japan Exchange Group)
- Nasdaq's LINQ (a platform for private market trading)

3.2.5 IDENTITY MANAGEMENT

It is of utmost importance that one has the ability to verify their identity on the Internet in order to make successful financial transactions online. In this context, we need to understand the following:

- Available remedies for the security risks connected with e-commerce are not exactly perfect.
- However, distributed ledgers offer improved methods to prove identity.
- Personal documents can be digitized.
- The company offering online transactions needs to have a good reputation.
- Universal online identity verification solution requires cooperation between private entities and the government.
- Different countries may pose various legal hurdles that need to be addressed and solutions found.

However, currently there is a solution that has been applied to e-commerce which relies on the SSL certificate (the little green lock) for secure transactions on the Internet. Work of creation of an SSL standard for blockchain is under process.

3.2.6 SMART CONTRACTS

It is possible to do the coding of simple contracts. These contracts can be executed when specified conditions are met. Ethereum has the potential to realise the possibility. Even now it is possible to do the following:

- Smart contracts can be programmed to perform simple functions.
- Payment of a derivative could be done with the use of Blockchain technology.
- Bitcoin payment could be automated.

(More on this in 3.5)

3.2.7 CROWDFUNDING

Blockchains have the potential to create crowd-sourced venture capital funds. This is the direct result of people wanting to have a direct say in product development.

3.2.8 EXAMPLES

- **Railway tickets:** When you buy a ticket online, the credit card company takes a cut for processing the transaction. If the entire ticketing process is moved to the blockchain, this processing fees can be avoided. It works like this:
  - The two parties in the transaction are the railway company and the passenger.
  - The ticket is a block.
  - This block is added to the chain.
  - It is a unique, independently verifiable record.
  - It is also a record of all transactions for, say, a certain route, or even the entire train network, comprising every ticket ever sold.

- **Ride-hailing or overnight stay:** Ride-hailing service such as Uber or Ola, or overnight stay facility such as Airbnb can save money on transaction fees by encoding the transactional information for a car-ride or an overnight stay.

This means that since blockchain transactions carry no transaction cost, one can charge for anything without third parties cutting into their profits.

3.3 USERS OF BLOCKCHAIN TECHNOLOGY

It is not easy to say who the users of blockchain technology are going to be as it is likely to affect a lot of systems and applications for our daily life. However, finance offers the strongest use cases for this technology.

They are the following:

- International remittances are likely to benefit most because of very high amounts of transaction done on a daily basis.
- Blockchain cuts out the middlemen for such transactions.
- The invention of Graphic User Interface (GUI) has made it possible for personal computing.
- The 'wallet' applications have been devised for the blockchain using GUI.
- The wallet helps people to buy things with Bitcoin and store.
- Wallet applications are likely to transform very soon to include other types of identity management. *(To some extent, it is happening even now.)*

3.4 BENEFITS OF BLOCKCHAIN TECHNOLOGY

Blockchain technology brings a wide range of value propositions for businesses. In fact, no sector should ignore it because it has the potential to ease various constraints currently existing in different business operations.

Blockchain technology has the capability to provide the following benefits:

- **Time reduction:** This will ensure quicker settlement of trades in terms of:
  - Verification process,
  - Settlement of claims,
  - Clearance.

- **Decentralised:** This helps because of the following:
  - There is no central authority;
  - There are standard rules governing the exchange of information by the nodes;
  - All transactions are validated;
  - All valid transactions are added one by one.

- **Reliability:** There is high degree of reliability because:
  - Identity of each participant is verified;
  - There is a procedure for removing double records;

- Rates are reduced;
- Transactions are accelerated.

- **Security:** The technology offers a high level of security because:
  - It uses advanced cryptography;
  - It is ensured that information is locked inside the blockchain;
  - It makes use of Distributed Ledger Technology;
  - A copy of the original chain is held by each participant;
  - Transactions through blockchain will not share any personal information regarding the participants;
  - It creates a transaction record by encrypting the identifying information;
  - It greatly reduces the possibilities of a data breach.

- **Unchangeable transactions:** The transactions done on blockchain are unchangeable because:
  - It registers transactions in a chronological order;
  - It is certified that operations are unalterable;
  - When a new block is added, it cannot be removed or modified.

- **Collaboration:** Every participant can make transactions with others directly. It means that they do not need any intermediary.

Fig. 3/1 shows the benefits of Blockchain Technology.

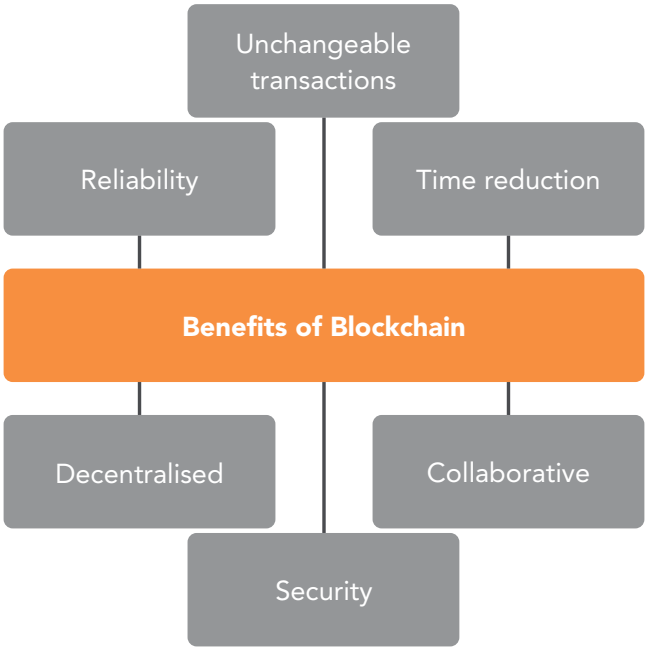

Fig. 3/1 Benefits of Blockchain Technology

3.5 SMART CONTRACTS

Blockchain has emerged as a disruptive force that is capable of affecting the world in myriad ways. This has been brought by smart contracts.

3.5.1 WHAT IS A SMART CONTRACT?

Smart contracts are pieces of code. They can be stored in a blockchain, and can be used to perform complex operations. We can say that it is a software which can self-execute. But it can do so only when one or more conditions are matched. We can also say that:

- It is a computer program that:
  - Can facilitate performance of an argument,
  - Uses blockchain technology.

- The process is automated;
- It can substitute for legal contracts;
- The terms of contract are recorded in lines of code.

The concept has been aptly described by Vitalik Buterin (b. 1994 - Vitaly Dmitriyevich 'Vitalik' Buterin, Russian-Canadian programmer and writer, co-founder of Ethereum and Bitcoin Magazine) in the following explanation:

> *"Suppose you rent an apartment from me. You can do this through the blockchain by paying in cryptocurrency. You get a receipt which is held in our virtual contract; I give you the digital entry key which comes to you by a specified date. If the key does not come on time, the blockchain releases a refund. If I send the key before the rental date, the function holds it releasing both the fee and the key to you and me respectively when the date arrives. The system works on the 'If-Then' premise and is witnessed by hundreds of people, so you can expect a faultless delivery. If I give you the key, I'm sure to be paid. If you send a certain amount in Bitcoin, you receive the key. The document is automatically cancelled after the time, and the code cannot be interfered by either of us without the other knowing, since all participants are simultaneously alerted".*

3.5.2 PROCESS OF SMART CONTRACT

There are certain steps that need to be followed for designing and publishing a smart contract.

They are:

- The contract has to be coded;
- The outcome has to be defined;
- The outcome is supposed to be triggered when the contract is executed;
- It has to be decided what conditions have to be matched for triggering the outcome;
- Once the contract has been published, each execution in every node in the system will achieve an individual agreement of its results;
- The network will then be updated, and which will show a record of the results of that execution;
- Now these results will be stored in the blockchain;
- After this, single party manipulation cannot be done.

3.6 BLOCKCHAIN PLATFORMS

Currently there are several blockchain platforms that provide the facility to integrate businesses using this technology. Some of these are mentioned below.

3.6.1 ETHEREUM

Ethereum is a platform which hosts smart contracts. It has been responsible for the appearance of various cryptocurrencies. We can further describe Ethereum in the following manner:

- It is an open source platform.
- It is based on blockchain technology.
- It allows developers to build and publish decentralised applications.
- It provides tools to build blockchain-based application in a streamlined way.
- It speeds up the process.
- It cuts down the difficulty level.
- It can host and run any application that has been built on it.
- Ether is used to pay for transactions fees and services on the Ethereum network.
- It can allocate any blockchain-based application created by the users.
- A computer can be effectively turned into a node of Ethereum's blockchain.

- It can host the development of thousands of different applications.
- It provides the ecosystem where smart contracts can substitute any centralised application.

3.6.2 HYPERLEDGER FABRIC

It is designed for permissioned networks, enabling known identities to participate within a system. The participants within this network should be authorised and should have credibility in the capital to take part in the blockchain.

3.6.3 HYPERLOGIC SAWTOOTH

It is an enterprise-grade and modular platform, designed for creating, deploying, and executing distributed ledgers which enable digital records to be maintained without a central authority.

3.6.4 HEDERA HASHGRAPH

It is a lightning secure, fast and fair platform that does not need to compute a heavy Proof-of-Work algorithm. It empowers and enables developers to build an entirely new class of decentralised applications that are scalable.

3.6.5 RIPPLE

It is aimed at connecting payment providers, digital asset exchanges, banks and corporates via a blockchain network, RippleNet, without any chargeback. It allows global payments through a digital asset called 'XRP or Ripple', which is now one of the popular cryptocurrencies like Ether and Bitcoin. Built on advanced blockchain technology XRP is more scalable and faster than other blockchains.

Several big brands are testing and planning to integrate the potential of Ripple's blockchain and planning to integrate it to make the existing payment process secure and faster. Some of these are:

- Santander
- American Express

- MoneyGram International
- SBI Holdings
- Deloitte

3.6.6 QUORUM

It is an enterprise-focused version of Ethereum. Unlike other blockchain platforms, it uses vote based and different algorithms to process hundreds of transactions per second.

3.6.7 HYPERLEDGER IROHA

It is a simple and modularised distributed ledger system based on a highly secure and fast consensus algorithm, protecting IROHA networks from adversary node or failures. The platform is highly applicable for supply chain and IoT uses.

3.6.8 CORDA

It enables institutions to transact directly with smart controls by removing costly frictions in business transactions. Corda does not have a cryptocurrency and is a permissioned blockchain platform which only allows the authorised participants to access the data, not the entire network.

Designed initially for the financial industry, for the financial sector, Corda is now being applied in various other uses cases like healthcare, trade, finance, supply chain, and government authorities. A large number of firms have invested more than $100 million into Corda, and are using it as a blockchain platform. Prominent among these are:

- Intel
- Microsoft
- HSBC
- Bank of America
- Merrill Lynch

3.6.9 EOS

It is designed for the development of dApps (Decentralised Applications). Its goal is to offer decentralised application's hosting, decentralised storage of enterprise solutions and smart contract capability, solving the scalability issues of Ethereum and Bitcoin.

3.6.10 OPENCHAIN

It is an open-source distributed ledger technology, highly suited for organisations willing to manage the digital assets in a secure and scalable manner.

3.6.11 STELLAR

Similar to Ripple, it can also deal with exchanges between cryptocurrencies and fiat-based currencies. It is possible to build banking tools, smart devices and mobile wallets using the Stellar network.

Stellar Consensus Protocol (SCP) makes it possible to reach consensus without depending on a closed system for recording financial transactions.

As compared to decentralised Proof-of-Work and Proof-of-Stake algorithms, Stellar Consensus Protocol (SCP) has modest financial and computing requirements, reducing the barrier to entry and opening up financial system to new participants.

Many companies are integrating with the Stellar network to enable money transfers across borders. Some of these are:

- TransferTo
- NaoBTC
- RippleFox
- ICICI Bank

3.6.12 DRAGONCHAIN

As a Service Platform it is designed to provide developers and enterprises the useful resources required to develop blockchain applications in minutes. Its public/private hybrid blockchain platform offers ease of use and high performance to develop and deploy blockchain apps and microservice-based smart contract.

4 BITCOIN AND DIGITAL CURRENCIES

4.1 INTRODUCTION

Digital currencies came into being because of Bitcoin and development of blockchain technology. The emergence of Bitcoin gave a new dimension to the use of advantages of digital currency. In fact, digital currencies are probably one of the most exciting and disrupting phenomena of modern times. Decision makers around the world have been greatly influenced with the emergence of an entire market worth billions of dollars volume.

4.2 ORIGIN AND DEVELOPMENT OF BITCOIN

Bitcoin was introduced in 2008 by an anonymous user, or a group of people, identified as Satoshi Nakamoto. In fact, the blockchain concept itself came into being on account of the Bitcoin initiative.

Let us see how it works:

- Bitcoin has a peer-to-peer structure;
- Bitcoins are transferred from user to user through the Internet;
- This transaction does not have to go through a bank or another financial institution;
- There is a huge reduction in transaction fees;
- There is a possibility of using Bitcoins in every country;
- There is a great case for its use in the banking sector as it could reduce their infrastructure cost by 30% - 40%.

4.3 ACCEPTANCE OF BITCOINS

Just like the conventional currencies, cryptocurrencies also face rise or downfall depending on the willingness of markets and countries to accept them and consider them a valid method of payment. In different countries, the governments have different approaches to cryptocurrency and Bitcoin in particular. There are countries where operations with cryptocurrencies are officially permitted, there are countries that negatively relate to this, but there are also completely neutral ones.

In this regard the following developments have come about:

- **Top 10 Bitcoin-friendly countries:**
  - Denmark
  - UK
  - Estonia
  - US
  - Sweden
  - South Korea
  - The Netherlands
  - Finland
  - Canada
  - Australia

- **Japan:** It has accepted Bitcoin as a legal method of payment since 2016.
- **Switzerland:** Financial institutions are allowed to conduct various transactions with cryptocurrency.
- **India:** Legally speaking, the use of Bitcoins is a grey area. The government has not regulated this form of currency, neither has it outlawed it. However, public are allowed to deal in Bitcoins (though with certain restrictions).
- **Russia:** It may not allow Bitcoin domestically but may allow for its use as a foreign currency.
- **China:** The situation is ambiguous, since it is forbidden to conduct operations with cryptocurrencies for banks, but it is allowed to individuals.
- Bitcoin is no more a mere concept, and has become a powerful currency affecting markets.
- After the success of Bitcoin other cryptocurrencies have also been developed (though all are based on blockchain technology). Some of these are:
  - Ether
  - Ripple
  - Litecoin
  - SolarCoin

4.4 FEATURES OF BITCOIN

Bitcoin's core value resides in the following features:

- It enables payments between users without the involvement of financial institutions.
- Peer-to-peer structure implies a huge reduction in transaction fees.

- Since there is no way to identify, track or intercept bitcoin transactions, taxes are not added to any purchases.
- Transactions are relatively faster than bank transfers in traditional currencies.
- Transactions are anonymous with no names involved.

4.5 DRAWBACKS OF BITCOIN

- It is an emerging currency and there is a lot of work yet to be done.
- Their value is highly volatile.
- Losing your private key can result in losing your bitcoins.
- Transactions cannot be reversed or cancelled.
- Governments may ban them any time.

5 DECENTRALISED APPLICATIONS

5.1 INTRODUCTION

All centralised systems are susceptible to be decentralised through the use of smart contracts such as the following:

- Loans provided by banks,
- Title registries,
- Voting systems,
- Regulatory compliance,
- Royalties for authors, artists, etc.

5.2 DECENTRALISATION THROUGH SMART CONTRACTS

Decentralisation can be achieved in various sectors. Some important ones are the following:

- **The energy sector:**
  - To issue payments between prosumers and consumers in ecosystems;
  - First group selling their excess energy to the second group;
  - Empowering consumers;
  - Encouraging competition;
  - Cutting down administrative costs;
  - Reducing time for issue of payment;
  - Linking the software to databases;
  - Linking sensors measuring various parameters such as wind speed or magnitude of earthquakes.

- **Patents and copyright:** A smart contract about ownership such as:
  - A song in the music industry;
  - Ownership over real estate.

- Keeping track of packages sent.

5.3 DECENTRALISATION APPLICATIONS

Blockchain-based applications are capable of replacing established processes. As far as Ethereum is concerned, it is an open software platform and enables deployment of decentralised applications. However, we need to understand what labels an application as decentralised.

To understand decentralised applications requires that we clearly define what they are. To achieve a decentralised status, an application has to meet the following criteria:

- It has to be open source;
- It must be autonomous;
- No single entity should be able to hold a majority of tokens;
- All potential changes must be executed only after obtaining consensus;
- The data and the protocols have to be cryptographically stored;
- The data should be stored in a blockchain;
- Cryptocurrencies or tokens are used to reward the users who support the network;
- New tokens are generated following a particular algorithm;
- This algorithm should be able to incentivise the users who contribute to the system.

Furthermore, we should analyse the following components to understand the degree of decentralisation achieved by an application.

These components are:

- **Architectural component:** We must identify:
  - The number of nodes (physical computers) that comprise a system;
  - The number of computers that break down and still the system remains operational.

- **Political component:** A huge number of entities control the computers that form the system. We must be able to identify the number of these:
  - Individuals; and/or
  - Organisations.

- **Logical component:** We must be able to distinguish whether the data is organised on:
  - A single structure; or
  - It consists of several independent units.

5.3.1 BENEFITS OF DECENTRALISATION

Decentralisation offers a number of benefits to the users because of its certain features.

They are:

- Decentralised networks have a high tolerance level;
- Attacking them is highly unfeasible;
- Attacking them is very expensive;
- One requires huge computing potential to attack them;
- Decentralisation acts as a barrier to collusion, and inhibits centralised corporations and governments from conducting businesses and operations in a non-transparent way;
- It is possible to code the set of rules and decision-making apparatus of an organisation, which means:
  - Eliminating the need for documents,
  - Eliminating the people governing it,
  - Creating a structure having decentralised control system.

In spite of these benefits of decentralisation, we need to give credence to the following statement made by Vitalik Buterin (b. 1994), founder of Ethereum:

> *"The highest degree is not always necessarily the most convenient for every case, and some applications may benefit for using a slightly more centralised approach".*

5.4 CONSENSUS MECHANISM

Blockchain is able to differentiate between legitimate and fake transactions, and that too, without the involvement of a centralised authority. This is achieved through a consensus mechanism.

It would be an ideal situation if everybody in the system is honest and will always remain so. But since obviously there may not be such an ideal situation, we need to understand the following:

- The algorithm can handle only a certain percentage of dishonest participants, and can still find the true version of the ledger. This is called Byzantine fault tolerance.
- The number of dishonest behaviours that the system can handle depends on the level of tolerance.

- It should be possible to use algorithm for reaching consensus at low operational level, failing which there will be no gain.
- The algorithm should be able to ensure that no parties cluster inside the system. If it happens, they may gain control over other users.
- The algorithm needs to discourage and disincentivize dishonest behaviours. This can be done by making them highly expensive.

5.4.1 POPULAR MECHANISMS

The following are the most popular mechanisms for achieving consensus:

- **Proof of Work:** It is a system of an economic measure. It is capable of deterring service attacks and other abuses such as spam on a network. It does so by requiring processing time by a computer. For Proof of Work the resource is computational power. To validate and store one set of transactions in the blockchain, huge amounts of computational power are required. This process works as follows:
  - The transactions get broadcasted to the miners (those who add transaction records to Bitcoin's public ledger);
  - The miners put them together in a group (block);
  - The miners need to find the correct hash (denoting size to a string of numerals and letters);
  - When a miner modifies the data, the hash of a block will change;
  - The miners add small packages of data (Nonce – 32-bit numbers);
  - Different Nonce values are tried and the hash is recomputed for value;
  - The finding of the block with the correct Nonce value results in a Proof of Work;
  - When a miner succeeds, the reward is then distributed among all the members of the mining pool;
  - Different mining pools compete against each other in mining each block.

However, Proof of Work has some weak points. The main one is that it requires a huge amount of energy. An estimated $1 million dollars' worth of electricity and hardware costs per day are burnt by both Bitcoin and Ethereum as part of their consensus mechanism.

In spite of this weakness, we can still say that proof-based consensus guarantees the following:

- Participation of the users in securing the system;
- Getting rewards from the algorithm users' participation;
- Increasing the speed of processing transactions;
- Disincentivizing malicious behaviours.

- **Proof of Stake:** Proof of Stake is an experimental concept. Its aim is to provide an equally safe consensus mechanism while addressing the flaws found in the system of Proof of Work. It works in the following manner:
  - In a chain-based Proof of Stake, one user is randomly selected as validator for each block;
  - Those with more funds at stake are automatically selected by the algorithm;
  - The system rewards for honest behaviour with newly generated coins.

- **Proof of Authority:** Proof of Authority (PoA) is an algorithm used with blockchains that deliver comparatively fast transactions through a consensus mechanism based on identity at stake. In PoA networks, transactions and block are validated by approved accounts, known as validators.

5.5 SECURITY

The Blockchain system is quite secure because:

- Azure Blockchain service uses several Azure capabilities to keep users' data secure and available;
- Data is secured using:
  - Isolation,
  - Encryption,
  - Authentication.

- Since blockchain is decentralised and immutable, the data is absolutely secure.

5.6 CHALLENGES AND BARRIERS

Blockchain is facing quite a few technical challenges. There are certain barriers to the safe implementation of this technology. We need to address these challenges and cross the various barriers. The following issues need to be addressed *(work is going on to solve some of these):*

- Bitcoin network requires a very high speed per second for its transactions. The capacity needs to be scaled up.
- Computational power has to be further increased.
- Security and privacy of blockchain solutions need further improvement.
- If both public key and private key of the user are lost, the account is vulnerable. So better solution is needed to ensure the safety of storing account data.

- Certain transaction patterns could uncover the key owner's identity. A solution for this needs to be found.
- The existing computing systems need to gradually change with regard to change of strategy and investment. This can be done with the involvement of the industry in a long-term perspective.
- There is a need for a cultural shift on the part of users and operators of these systems.
- It is the need of the hour for the governments to come out with clear regulations which will trigger the massive adoption of blockchain technology. This needs to be done in order to:
  - Avoid incurring in-market failure;
  - Ensure a minimum standard of product quality for the consumers.

Moreover, this technology is evolving so fast that it is hard to delimit the scenario where the regulation will become effective. Hence, before regulators can create a legal framework, they must reach a better understanding of the technology and its impact.

International Organisation of Securities Commission (IOSCO, 2019) has published a consultation focusing on how platforms which trade crypto-assets are regulated. The global standards-setting body considers that promoting innovation must be balanced with appropriate regulatory oversight.

In its report it has stated that:

> *"Financial technology regulators may need to develop 'highly automated' surveillance and hire technology experts if they want to closely monitor risks posed by blockchain".*

The report has further stated that:

> *"The global nature of Fintech therefore creates challenges that regulators should address through international cooperation and the exchange of information".*

We can safely say that:

> *"Any technology that is developed today starts affecting the existing systems and practices throughout the world, and blockchain is no exception. Hence global regulation is required for this global technology at the earliest".*

6 DEVELOPMENT OF BLOCKCHAIN TECHNOLOGY

6.1 INTRODUCTION

The blockchain technology is one of the latest technological revolutions. It is a technology, people believe, which has the potential to change the world. It is the backbone of Bitcoin – the now infamous (to some) cryptocurrency. It is believed that since it is a 'distributed ledger' it can be trusted for its safe and secure transactions.

6.2 DEVELOPMENT OF BLOCKCHAIN

It is believed that a decade from now, it is more likely than not that the blockchain will be embedded in our daily lives in ways that we cannot even imagine today. The various companies and governments have already spent billions of dollars in blockchain technology. Fortune 500 companies are investing billions in the blockchain. Businesses are using the distributed ledger technology behind Bitcoin to track their supply more efficiently. Businesses are beginning to adopt blockchain technology to track their supply chain more efficiently.

Blockchain technology creates a record of each spot it has been in, making it useful for the enterprise, especially in the shipping industry.

Blockchain, the distributed ledger technology that supports Bitcoin and other cryptocurrencies, is being increasingly adopted for enterprise use.

Since it creates and maintains a permanent transcript of an item's transactions, blockchain technology can be helpful for tracking a company's supply chain. Using the emerging technology instead of past methods could be more efficient and accurate, saving businesses time and money.

Here are some companies experimenting with using blockchain to drive their supply chain:

- Walmart
- Maersk
- British Airways
- UPS
- FedEx

Some others are these:

- IBM
- Accenture
- PwC
- JP Morgan Chase

Some companies have announced – and are already in the process – investment in blockchain technology. Two of these are:

- Silicon Valley venture capitalists
- Andreessen Horowitz

Some of the countries that are starting work with blockchain technology are the following:

- England
- Singapore
- India
- South Korea
- Ukraine
- UAE
- Kuwait
- Netherlands, and many more.

Marc Andreessen (b. 1971), who is credited with inventing the modern Web browser, announced – on behalf of his company Andreessen Horowitz – a $300 million "crypto" fund to exclusively invest in blockchain technology. While introducing the fund, Andreessen and his colleagues said that:

> *"For those of us who have been involved in software for a long time, it feels like the early days of the Internet, Web 2.0, or smartphones all over again".*

This explanation of where this new technology sits within history feels right. We may go on talking about crypto and blockchain as a bubble, it is likely just early days. And while 1999 marked what seemed like a high point for the Internet before a precipitous fall, it proved to only be the first stage of its rise.

As far as blockchain is concerned, there may be failures, misspent money and scams, but a decade from now, when we look back a few years, it is more likely than not that blockchain will become an integral part of our life.

6.3 PROSPECTIVE USES

The blockchain is, of course, being used to create all sorts of cryptocurrencies, led by Bitcoin and Ethereum. But what is more important is that it is touching all different industries. Various industries are planning to use blockchain.

Some of these are the following:

- The advertising industry plans to use it to track advertisements on the Internet.
- The music industry is planning to use it to track songs.
- Banks and mortgage companies want to use it to track the deeds of homes and the complex process of tracking all the documentation.
- Shipping companies are investing in blockchain technology to track bills of lading.
- The pharmaceutical industry wants to use the technology to verify the drug supply chain.

It is believed that blockchain technology may bring a new level of enhanced trust to business and may also cut out the middlemen that have historically tracked – and profited – from the complexity of so many different systems trying to communicate with each other. That could lower prices for goods and services.

Blockchain is about solving society's ultimate challenge: trust, or rather, lack of trust. It is about using technology to create a shared sense of trust in a group of disparate participants.

Some people believe that blockchains are used only to record virtual currency transactions. But it is not so. Though most of the early efforts to imitate the Bitcoin blockchain were done by programmers looking to create virtual currencies with slightly different features from Bitcoin, over time some of these new virtual currencies added on significant new features that updated the blockchain concept so it could handle more kinds of information.

Recently, many companies and governments have been interested in using blockchains to store data that has nothing to do with transactions of any sort. While banks are building blockchains that can track payments between accounts, governments are experimenting with using blockchains to store property records and votes.

A lot of companies are excited about blockchain technology. They have experienced that there are several limitations that come with the old ways of keeping data, with a single authority responsible for all the updates. If that authority gets compromised by a hacker, or even by natural disaster, the people relying on that database can lose access to all their data. With a blockchain, all the people relying on the database can keep and update their own copy of the data.

6.4 POWERING ONLINE TRADE

Blockchain allows conducting multi-party coordination steps based on different document validations. Many companies have launched blockchain platforms. Given below are two significant platforms:

- TigerTrade, and
- TradeFlo.

These two are changing the ways of international trade. While TigerTrade is a step towards organising buying and selling of excess inventory, TradeFlo goes a step further to facilitate global trade through blockchain.

6.4.1 TIGERTRADE

TigerTrade was created by Tanjila Islam in 2010 in New York. This online platform has a huge number of manufacturers and buyers on board and is the largest marketplace for buying and selling excess retail inventory.

TigerTrade boasts of the following advantages:

- It enables buyers and sellers from across the globe to transact safely, efficiently, and with full transparency;
- It sources only the best fashion stockists of in-demand merchandise at every price point;
- It manually vets each member of its marketplace so that members can transact with complete confidence;
- It has been able to organise the highly unorganised secretive business of excess inventory.

6.4.2 TRADEFLO

Soon after launching TigerTrade, Tanjila realised that there were several challenges as a lot of paperwork was involved in import and export. The team was investing a lot of time and effort in the business but was not seeing it scale as fast as it wanted to.

She says:

> *"We realised that despite being an online trade platform, due to the tedious paper work, a lot of the work had to be done offline".*

She found the solution in blockchain, and consequently TradeFlo was born in 2018 in San Francisco. And suddenly the business started moving forward much quickly.

Tanjila was initially designing the platform only for TigerTrade, but soon realised that such a platform could be utilised by many more companies across the globe. Powered by smart contracts, the platform ensured security and trust.

TradeFlo is a supply chain, trade, and structured finance facilitation platform that connects Latin American corporates and exporters with bank, non-bank, alternative, and traditional financing sources based in the Americas, Europe and Asia.

Their solutions provide companies with short, medium and long-term financing alternatives which could be applied to supply chain, trade finance and bespoke assets financing.

TradeFlo works in the following manner:

- It creates validated vendor identity;
- Once that gets created, it allows storage and sharing of:
  - Purchase orders,
  - Invoices,
  - Implementation documents, etc.

- It enables tracking of such orders;
- It allows sharing of data on real-time basis with multiple permission parties.

TradeFlo can bring the following advantages:

- Helps companies create validated vendor profile which in turn allows them build trusted relationships with new buyers quickly;
- This 'risk profile' helps in turn get:
  - New buyers,
  - Better payment terms,
  - Access to financing.

- Decreases transaction and coordination costs for:
  - Payments,
  - Inspection,
  - Shipping,
  - Risk management.

- Increases transparency;
- Improves overall efficiency;
- Focuses on each and every part of a transaction.

7 PROSPECTS OF BLOCKCHAIN TECHNOLOGY

7.1 INTRODUCTION

The key challenges of using blockchains in industries other than financial services sector are the following:

- The lack of awareness and understanding of the blockchain concept;
- Lack of knowledge how it works;
- Lack of technical understanding;
- Hesitation in making a cultural shift from the traditional ways of doing things;
- Reluctance to adopt decentralisation of the whole process;
- Complying with existing regulations;
- Ensuring the required data privacy and security for the shared databases.

7.2 PROSPECTS

The global business entities are yet to explore the intricacies of the blockchain concept to its fullest. However, it is believed that with the ongoing researches and experiments, the day is not far off when blockchain will become an integral part of our daily life.

7.2.1 CURRENT USES

There are many applications which work on the principles of blockchain technology, and which are being used in some measure. Some of these are:

- Abra is providing remittance payments based on a blockchain solution. It advertises its services for 2% while conventional methods charge around 7%.
- Many banking and financial institutions such as Santander, UBS, UniCredit have joined Ripple to being able to offer global financial settlement solutions based on blockchain with the cryptocurrency.
- GE Aviation uses blockchain to streamline tracking of aircraft parts from factory to flight.

- Buhler uses blockchain technology to track crops from farm to fork, keeping food healthy and safe for billions of people every day.
- 3M uses Azure Blockchain to enable a new label-as-a-service approach for securing its supply chains.
- Nasdaq brings blockchain technology to capital markets to manage transaction delivery, payment and settlement from multiple blockchains and payment mechanisms.
- Microsoft uses blockchain solutions to compute royalty statements for Xbox game publishers in hours, instead of months.

7.2.2 POTENTIAL USES

New business models can be developed taking into account incentives for providing information. We can think of these platforms as a means to reduce service costs for small customers of a single company.

There could be other potential uses. They are:

- Since blockchain has the transparency and data traceability, it can provide the platform to include AI (Artificial Intelligence) for smart contracts optimizing the value of physical assets. A drone could be independently taking the best orders, self-deciding when to go for repair and fly at the end of its life to a recycling place.
- We can think of blockchain as the means to unfold the potential of Industry 4.0.
- The potential of the combination of Industry 4.0, blockchain, and AI (Artificial Intelligence) with big data especially, can help to reduce risks and tailor documents such as insurance or maintenance contracts to improve the quality standards of society, and organisations such as public notaries and banking services will have the willingness to test and build blockchain applications.
- In energy markets, the Energy Web Foundation from the Rocky Mountain and Grid Singularity, aims to establish a platform for blockchain-based energy services. In 2019 Energy Web (EW) launched the Energy Web Chain, the world's first open-source, enterprise blockchain platform tailored to the energy sector. EW focuses on building core infrastructure and shared technology, speeding adoption of commercial solutions, and fostering a community of practice. The EW Chain is a public blockchain network open to all utilities, users, and devices. With a virtual machine identical to public Ethereum, developers can begin writing smart contracts and dApps (Decentralised Applications) with little to no additional learning curve. The enterprise-grade

EW Chain boasts high scalability, low transaction costs, and lean energy consumption, thanks to its permissioned Proof-of-Authority consensus.

- While connecting generation assets and consumers of energy with smart gateways, we can create a platform where services can be booked like an app. Other services might be P2P (Peer-to-Peer) trading or balancing demand and supply. In these platforms, blockchain technology offers the opportunity to own one's data and to parts of it.

In the future, blockchain applications will gain prominence, and it will be important for the whole management board – not only finance and I.T. functions – to understand their potential benefit.

7.3 NEW CAREERS

The latest development in the job market is the emergence of blockchain as the most disruptive career option. The blockchain technology is often touted as the 'new Internet' by most businessmen and entrepreneurs. They had been seeing blockchain as a safe and secure way for transaction, and now, have begun considering it as the most disruptive career option too.

Several businesses are inclined towards making blockchain an integral part of their business. Companies are looking forward to the blockchain technology. Blockchain has sprouted several new career opportunities. Some of the top jobs in blockchain environment are the following:

- **Blockchain developer:** They design the architecture of blockchain systems and are needed to help build products and services associated with the technology, like contracts and apps. To be a blockchain developer, one needs skills such as:
  - Hyperledger,
  - Node.js,
  - Smart contract,
  - Eye for detail.

- **Blockchain quality engineer:** They are responsible for testing and ensuring quality control in blockchain development.
- **Blockchain attorney or legal consultant:** Companies need their legal expertise while launching blockchain technologies to understand the implications of how business and finance are managed, besides tracking and confirming transactions, particularly in the modern times.

7.3.1 UPSKILLING

The demand for blockchain developers and project managers is very high, but availability of talent that can guide start-ups is very limited. This situation requires that those with good computer knowledge and expertise upskill themselves to meet this demand.

Upskilling in blockchain technology will be beneficial in the following way:

- It is relevant for coders who could look to build blockchain products. They need to have coding experience, preferably in Java, and a good sense of mathematics. It is also essential to have knowledge of:
  - the foundational development aspects of Ethereum, Hyperledger Fabric and Composer, and
  - functional aspects (hands-on projects and case studies).

- It is relevant for tech managers, project managers, and tech architects looking at product development and architecting solutions.
- It is relevant for banking and finance, legal and other professionals who are evaluating use cases for Blockchain application.

GLOSSARY

Bitcoin

It is a digital currency that is not backed by any country's central bank or government. Bitcoin can be traded for goods or services with vendors who accept Bitcoins as payment.

Blockchain

It is a new paradigm of organisation. It is an incorruptible ledger that allows users to establish connections without the need of a middleman or third party, and recording all transactions in a decentralised database.

Byzantine fault tolerance

It means maximum percentage of dishonest participants that an algorithm can handle while still finding the true version of a shared ledger.

Cryptocurrency

A cryptocurrency is a digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets.

Consortium Blockchain

A consortium blockchain is a blockchain in which the consensus process is controlled by a pre-selected set of nodes. The right to read the blockchain may be public, or restricted to the participants. These blockchains may be considered 'partially decentralised'.

Digital signature

It is a digital code which is attached to an electronically transmitted document to verify its contents and the sender's identity.

Double spending

A double spend is an attack where the given set of coins is spent in more than one transaction. There are a couple main ways to perform a double spend: send two conflicting transactions in rapid succession into the Bitcoin network. This is called 'race attack'.

DAO (Data Access Object)

DAO (Data Access Object) is an organisation that is run through rules encoded as computer programs called smart contracts. A DAO's financial transactions record and program rules are maintained on a blockchain.

Ether

Ether is, like Bitcoin, a digital asset that does not require a third party to approve a transaction. It is a form of payment made by the clients of the Ethereum platform.

Ethereum

Ethereum is an open-source, public, blockchain-based distributed computing platform featuring smart contract functionality. It provides a decentralised virtual machine, the Ethereum Virtual Machine (EVM), which can execute scripts using an international network of public nodes.

Hash

It is a cryptographic hash function which takes an input (or 'message') and returns a fixed-size alphanumeric string. The string is called the 'hash value'.

ICO

It stands for Initial Coin Offering. It is an unregulated means of crowdfunding via the use of cryptocurrency, which can be a source of capital for start-up companies.

Industry 2.0

It is the transformation which was brought about by the introduction of electricity in the various processes.

Industry 4.0

It is the trend towards automation and data exchange in manufacturing technologies and processes which include Cyber-Physical Systems (CPS), the Internet of Things (IoT), Cloud Computing and Artificial Intelligence (AI).

Litecoin

Litecoin has largely been described as the 'silver' to Bitcoin's 'gold'. It appeared two years after Bitcoin (2011), improving some technical aspects like the average time necessary to process a transaction. Its value proposition is the same.

Mining

Mining is the process of adding transaction records to Bitcoin's public ledger of past transactions.

Nonce

The 'nonce' in Bitcoin block is 32-bit (4-byte) field of which the value is set so that the hash of the block contains a run of leading zeros.

Peer-to-peer (P2P)

A P2P (Peer-to-Peer) architecture divides tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.

Proof of Stake

Proof of Stake (PoS) concept states that a person can mine or validate block transactions according to how many coins they hold. This means that the more coins owned by a miner, the more mining power they have.

Proof of Work

A Proof of Work (PoW) system is an economic measure to deter denial of service attacks and other service abuses such as spam on a network, by requiring some work from the service requester, usually meaning processing time by a computer.

Proof of Authority

Proof of Authority (PoA) is an algorithm used with blockchains that deliver comparatively fast transactions through a consensus mechanism based on identity at stake. In PoA networks, transactions and block are validated by approved accounts, known as validators.

Public Blockchain

A public blockchain is a blockchain that anyone in the world can read, anyone in the world can send transactions to and expect to see them included if they are valid, and anyone in the world can participate in the consensus process. These blockchains are generally considered to be 'fully decentralised'.

Private Blockchain

A fully private blockchain is a blockchain in which writing permissions are kept centralised for a single organisation. Reading permissions may be public or restricted to an arbitrary extent.

Ripple

Ripple is a digital currency that utilises blockchain technology and the concept of digital tokens to simplify global banking. Major banks and financial institutions can adopt Ripple's system and use it to effectuate economic transactions in a more efficient way.

SolarCoin

SolarCoin is an alternative digital currency that provides an incentive to produce more solar electricity globally, by rewarding generators of solar electricity. SolarCoin is intended to shift the cost of electricity, thereby reducing the payback time of a solar installation.

Smart contract

A smart contract is a computer protocol intended to facilitate, verify, or enforce the negotiation or performance of a contract. It is a software with the ability of self-executing when one or more conditions are met.

REFERENCES

- Andreessen, Marc, *Why Bitcoin matters*, New York Times, Jan 22, 2014, Retrieved from: https://coindesk.com/mac-andreessen-believes-bitcoin.
- Buterin, Vitalik, *Ethereum*, 2015, Retrieved from: https://ethereum.org
- Energy Web Foundation, *The EW Chain*, 2019. Retrieved from: https://energyweb.org/technology/energy-web-chain/
- International Organisation of Securities Commission (IOSCO), *Consultation about crypto assets*, 2019, Retrieved from: https://blockchain.bakermckenzie.com.
- Mougayar, William, *The Business Blockchain*, Wiley, 2016.
- https://www.trade-flo.com
- Takyar, Akash, *Top Blockchain platforms of 2020*, Retrieved from: https://www.leewayhertz.com/blockchain-platform-for-top-blockchain-companies