

CONCEPT PAPER
ON
BLOCKCHAIN TECHNOLOGY
ADOPTION TRENDS AND IMPLICATIONS
FOR ACCOUNTANCY PROFESSION
2018



Digital Accounting and Assurance Board

**The Institute of
Chartered Accountants of India**

(Set up by an Act of Parliament)



CONTENTS

INTRODUCTION	3
FOREWORD	4
PREFACE	6
1. WHAT IS BLOCKCHAIN?	7
1.1 Introduction	7
1.2 History	8
a. Shortcomings of current transaction systems	8
b. Evolution of Blockchain	9
1.3 How Does It Works	10
a. Participants and their roles	10
b. Key Concepts	10
1.4 Benefits	15
a. Efficiency	16
b. Cost Effective	16
c. Enhanced Privacy	16
d. Transparency	16
e. Governance and Trust	17
2. WHY BLOCKCHAIN IS A DISRUPTIVE TECHNOLOGY	18
2.2 Risk For Adoption of Blockchain Technology	18
2.3 Building Trust With Blockchain	20
3. CURRENT USAGE OF BLOCKCHAIN	21
3.1 Financial Applications	21
a. Private Securities	21
b. Insurance	22
c. Government	22
d. Automotive	23
e. Manufacturing	23
f. Banking	24
3.2 Non-financial Applications	24
a. Supply Chain Management	24
b. Healthcare	24
c. Global Logistics and Shipping	25
d. Notary Public & Deed Records	25
e. Music Industry	26
f. Decentralized Proof of Existence	26

g.	Decentralized Storage	26
h.	Decentralized IoT	27
l.	Anti-Counterfeit Solutions	27
j.	Internet Applications	27
k.	Retail/E-Commerce	28
l.	Others	28
4.	ACCOUNTING ASPECT OF BLOCKCHAIN	29
4.2	Potential to Enhance Accounting System	29
4.3	Skills for the Future	29
4.4	How Accountancy Profession Can Lead in Blockchain Landscape	30
5.	ASSURANCE OF BLOCKCHAIN BASED SYSTEM / PROCESSES	31
5.1	Impact of Blockchain on Audit / Assurance	31
5.2	Future Roles of Chartered Accountants In Blockchain Ecosystem	32
a.	Audit of Smart Contracts	32
b.	Service Auditor of Consortium Blockchain	32
c.	Central Access Granting Administrator	32
d.	Arbitration Function	32
6.	ADOPTION AND THE PHASES OF DEVELOPMENT	34
6.1	Phase I: Early Adoption by Accounting Firms	34
a.	Accounting firms have already started research on Blockchain	34
6.2	Phase II: Approaching Mainstream Adoption (Critical Mass in 3-5 Years)	34
a.	Streamlining internal accounting practices and processes	34
b.	Real-time Audit trail & Assurance	34
c.	Smart Contracts, Supply chain management & Real-time analytics	35
d.	Taxation & Revenue Recognition	35
e.	Cost Saving	35
6.3	Phase III: Global Adoption (maturity By 2025)	36
	CASE STUDIES	37
Case Study 1:	R3 - Interbank Reconciliation	37
Case Study 2:	Land Registry	37
Case Study 3:	IBM Hyper Ledger	38
Case Study 4:	Dole Food Company, Inc.	38
	CONCLUSION	41
	REFERENCES	42

INTRODUCTION

The Institute of Chartered Accountants of India (ICAI) is a statutory body established by an Act of Parliament, viz. , The Chartered Accountants Act, 1949 (Act No. XXXVIII of 1949) for regulating the profession of Chartered Accountancy in the country. ICAI is the one amongst accountancy bodies in the world, with a strong tradition of service to the Indian economy in public interest.

Over a period of time, ICAI has achieved recognition as a premier accounting body not only in the country but also globally, for maintaining highest standards in technical, ethical areas and for sustaining stringent examination and education standards. Since 1949, the Chartered Accountancy profession in India has grown leaps and bounds in terms of:

- Members and student base
- Regulate the profession of Accountancy
- Education and Examination of Chartered Accountancy Course
- Continuing Professional Education of Members
- Conducting Post Qualification Courses
- Formulation of Accounting Standards
- Prescription of Standard Auditing Procedures
- Laying down of Ethical Standards
- Monitoring Quality through Peer Review
- Ensuring Standards of performance of Members
- Exercise Disciplinary Jurisdiction
- Financial Reporting Review
- Input on Policy matters to Government.

Digital Accounting And Assurance Board of ICAI

ICAI has constituted “Digital Accounting and Assurance Board” (DAAB) for fostering a cohesive global strategy on aspects related to digital accounting and assurance, through sharing of knowledge and practices amongst the members. DAAB is endeavouring to identify, deliberate and highlight on issues in accounting (including valuation) and assurance (including internal audit) issues in the digital world.

DAAB is focusing on issues in accounting and assurance arising from the high pace of digitisation, including use of artificial intelligence in audit, big data analytics in audit, relevance of sampling, valuation of data as an asset, impairment testing of digital assets, insurance of data - valuation and premium fixation, etc. The Board is taking up initiatives to develop knowledge base through position papers and articles on issues relating to impact of technology on accounting and assurance.

Initiatives to position the profession for opportunities in digital era are:

- Conducting Scalable, Employable and Updated Post Qualification Course on Information System Audit (DISA)
- World Class Training to Members on Forensic Accounting and Fraud Detection (FAFD)
- Imparting Hands on Training through Forensic Labs
- Evolving firms into thriving digital practice by providing leading technology solutions
- Research on Emerging Technologies - Artificial Intelligence, Cloud Computing and Robotics
- Executive Development Program on “Blockchain Technology – Driver of Digital Era”
- Capacity building in digital ecosystem of stakeholders including banks, PSUs
- Mentoring of Technology Driven Startups by Chartered Accountants
- Team of Innovators for helping members navigate digital path
- Digital Competency Maturity Model for upgrading firms in digital landscape
- Research Paper on “Early Signals on Fraud in Banking Sector”
- Incubation Centre for Blockchain Technology
- Webinars on strategies and approach to adopt technology in assurance services
- Research on embedding the understanding and use of technology in accounting and assurance services.

FOREWORD

Worldwide emerging technologies are going mainstream and drastically changing business landscape. Blockchain is one such revolutionary technology, and Indian government in the 2018 Union Budget has shown interest in exploring use of blockchain technology proactively for ushering digital economy. Decentralized ownership, immutability, cryptographic security are unique features of blockchain leading to more secure, transparent and efficient processes. Not just the businesses but such technologies are having great impact on professionals as well. It is right time that all professionals including Chartered accountants must leverage blockchain technology by accelerating efforts for implementation of this nascent technology in their professional work.

This Concept Paper on “**Blockchain Technology - Adoption Trends and Implications for Accountancy Profession**” issued by Digital Accounting and Assurance Board (DAAB) of ICAI, is an endeavour to provide overview of current blockchain-related practices, significant milestones in this technology's emergence, and introduction of possible new services and roles for professional accountants.

I compliment CA. Atul Kumar Gupta, Chairman, DAAB, and CA. Manu Agrawal, Vice-Chairman, DAAB, and other members of the Board for taking up this initiative for the benefit of profession. I am confident that our members would take benefit of this publication, and will make tangible progress in embracing blockchain technology in their professional work.

CA. Naveen N. D. Gupta
President, ICAI

New Delhi
August 03, 2018

In this phase of massive Digital transformation, Blockchain technology is unique and the most innovative one. Governments, regulators, banks and corporates around the world are poised to experiment with multiple blockchain prototypes so as to customise this emerging technology to fit multiple use cases.

As a proactive initiative, Digital Accounting and Assurance Board has released Concept Paper on “**Blockchain Technology - Adoption Trends and Implications for Accountancy Profession**” which examines current macro trends of blockchain ecosystem and analyses impact of the technology on various industry/ sectors. The focus is to identify the implications of the Blockchain technology on accountancy profession, and develop a way forward to evolve current practices of Accounting, Assurance and Advisory.

I am sure that this Concept Paper will give a rich insight to our members for moving ahead in the revolutionary Blockchain landscape.

CA. Prafulla P. Chhajed
Vice-President, ICAI

New Delhi
August 02, 2018

PREFACE

Blockchain is a revolutionary technological innovation offering immense potential for re-engineering economic models to deliver productivity gains to multiple industries, from financial sector to energy markets, intellectual property management, supply chains, public sector, and beyond. Implementing new infrastructure in blockchain landscape will require collaborative action to bring about changes to existing regulations, standards of practice, and creation of new legal and liability frameworks.

Chartered Accountants can prove to be a powerful catalyst for adoption of blockchain-based financial solutions by organisations, that can provide basis for a technological leap. Considering this, Digital Accounting and Assurance Board (DAAB) of ICAI has released “Concept Paper on Blockchain Technology - Adoption Trends and Implications for Accountancy Profession”. This document briefly explains fundamental concepts and unique features of blockchain technology, highlighting current usage of this novel technology. It throws light on accounting and assurance of blockchain based systems/ processes, and also adoption and development phases by accounting firms. Case studies have been included for explaining practical aspects to the readers.

We would like to place on record our sincere gratitude to CA. Tushankur Saroha, Convenor of the Group, CA. Sagar Arora and other members of the Group for their contribution in preparation of draft of this important publication of the Board.

We would like to express our gratitude to CA. Naveen N. D. Gupta, President ICAI and, CA. Prafulla Premeek Chhajed, Vice President, ICAI for their thought leadership, continuous support and encouragement to the initiatives of the Board. We are also thankful to all Board members, co-opted members and special invitees for their invaluable guidance and support to various activities of the Board. We would like to thank CA. Jyoti Singh, Secretary, DAAB, for her inputs and efforts in finalizing this Concept Paper.

We hope that the members and other interested readers would find this Concept paper of immense use in understanding this nascent technology, thereon driving its adoption in organizations.

CA. Atul Kumar Gupta
Chairman, DAAB

CA. Manu Agrawal
Vice-Chairman, DAAB

New Delhi
July 31, 2018

Chapter 1

WHAT IS BLOCKCHAIN?

1.1 Introduction

Blockchain came to prominence in the popular media recently. Articles ranged from distrust that Blockchain are nothing more than shared databases hyped up by venture capitalists, to amazement and wonder about a new technology that has the potential to create social, societal, and economic change.

So far, the focus of the discussion around this technology has centred on Blockchain used as a tool for financial services to improve transparency and efficiency and reduce cost within the industry. In response, Blockchain technology providers are being created all over the world, incubated independently or by innovation labs sponsored by banks and other entities. Start-ups are enthusiastically experimenting on applications of this technology to problems within the financial services domain.

It has been said that Blockchain will do for transactions what the Internet did for information. What that means is that it allows increased trust and efficiency in the exchange of almost anything. Blockchain can profoundly change how the world works. As described by the World Economic Forum, it is the future “beating heart” of the financial sector.

Blockchain, most simply defined as a shared, immutable ledger, has the potential to be the technology that redefines those processes and many others. To be clear, when we talk about Blockchain, we are not talking about bitcoin. Bitcoin, a crypto currency that emerged in 2009, provided the first widespread use of blockchain. But the reaches of Blockchain extend far beyond the introduction of crypto currencies.

Blocks in a chain = pages in a book: For analogy, a book is a chain of pages. Each page in a book contains the text and information about itself: at the top of the page there is usually the title of the book and sometimes the chapter number or title; at the bottom is usually the page number which tells you where you are in the book.

'Blockchain Technology' means different things to different people, and it can be confusing. Most of the time it is about distributed ledgers, i.e., a list of transactions that is shared among several computers, rather than being stored on a central server.

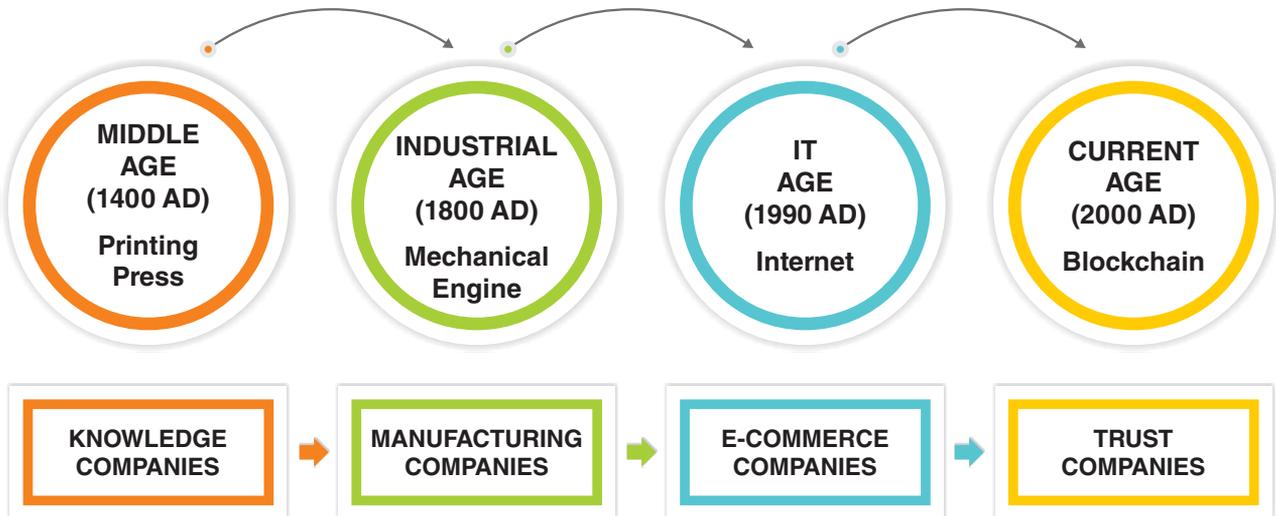
Commonly, it is **storage of data** that:

- Usually contains financial transactions;
- Is replicated across several systems in almost real-time;
- Usually exists over a peer-to-peer network;
- Uses cryptography and digital signatures to prove identity, authenticity and enforce read/write access rights;
- Can be written by certain participants;
- Can be read by certain participants, or a wider audience; and
- Have mechanisms to make it hard to change historical records, or at least make it easy to detect when someone is trying to do so.

The idea behind Blockchain, in short, is to be able to establish and verify trust without the need of a

centralized system. Instead, this power would be given to a decentralized network, making it not only more secure but also both more efficient and faster to scale. **This technology is still new, but the potential impact it can have on business and finance is exciting, and immense.**

1.2 History



a. Shortcomings of current transaction systems

Throughout history, instruments of trust, such as minted coins, paper money, letters of credit, and banking systems, have emerged to facilitate the exchange of value and protect buyers and sellers. Important innovations, including telephone lines, credit card systems, the Internet, and mobile technologies have improved the convenience, speed, and efficiency of transactions while shrinking and sometimes virtually eliminating the distance between buyers and sellers. Still, many business transactions remain inefficient, expensive, and vulnerable, suffering from the following limitations:

- Cash is useful only in local transactions and in relatively small amount;
- Time between transaction and settlement can be long;
- Duplication of effort and the need for third-party validation and/or the presence of intermediaries add to the inefficiencies;
- Fraud, cyber-attacks and even simple mistakes add to the cost and complexity of doing business, and they expose all participants in the network to risk if a central system, such as a bank, is compromised;
- Credit card organizations have essentially created walled gardens with a high price of entry. Merchants must pay the high costs of on boarding, which often involves considerable paperwork and a time-consuming vetting process;
- Half of the people in the world don't have access to a bank account and have had to develop parallel payment systems to conduct transactions.

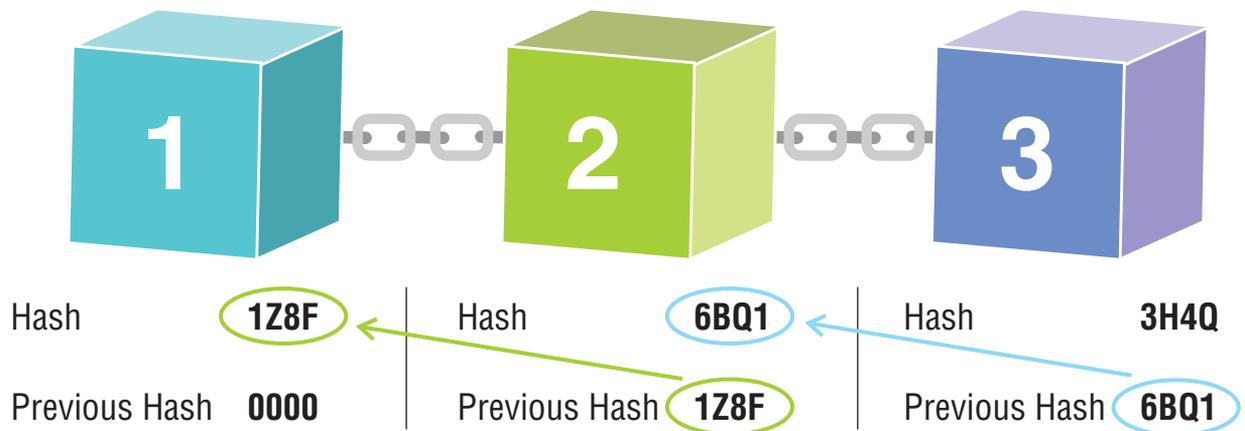
Transaction volumes worldwide are growing exponentially and will surely magnify the complexities, vulnerabilities, inefficiencies, and costs of current transaction systems. Growth of e-commerce, online banking, and in-app purchases, and the increasing mobility of people around the world have fuelled the growth of transaction volumes.

To address these challenges and others, the world needs networks that are fast and that provide a mechanism that establishes trust, requires no specialized equipment, has no chargebacks or monthly fees,

and provides a collective bookkeeping solution for ensuring transparency and trust.

b. Evolution of Blockchain

In the year 2008, an individual or group writing under the name of Satoshi Nakamoto published a paper entitled “Bitcoin: A Peer-To-Peer Electronic Cash System.” This paper described a peer-to-peer version of the electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution. Bitcoin was the first realization of this concept. Now word cryptocurrencies is the label that is used to describe all networks and mediums of exchange that uses cryptography to secure transactions-as against those systems where the transactions are channelled through a centralized trusted entity. The author of the first paper wanted to remain anonymous and hence no one knows Satoshi Nakamoto to this day. A few months later, an open source program implementing the new protocol was released that began with the Genesis block of 50 coins. Anyone can install this open source program and become part of the bitcoin peer-to-peer network. It has grown in popularity since then.



Data-->hash-->hash Of The Previous Block

The popularity of the Bitcoin has never ceased to increase since then. The underlying Blockchain technology is now finding new range of applications beyond finance.

BLOCKCHAIN TIMELINE

October 2008:
Bitcoin whitepaper by the nom-de-plume Satoshi Nakamoto is published.

May 2010:
First Bitcoin purchase: BTC 10k for a \$25 pizza. Today BTC 10k is worth \$10m! Bitcoin is known as the first use case of Blockchain technology.

June 2014:
LHV pank starts research on Blockchain and its digital security with their app "Cuber Wallet"

July 2014:
Ethereum Project - a Blockchain platform with the ability to build decentralized applications - is funded by a crowd sale.

September 2015:
Major financial companies form R3 - a consortium of over 40 institutions committed to exploring and implementing Blockchain technology.

September 2015:
Visa, Citi, Nasdaq Capital One and Fiserv invest \$30m in the Blockchain startup Chain.com.

September 2016:
Over 40 financial service institutions have invested in a Blockchain or Bitcoin startup since 2014.

2018:
WEC estimates that 80% of all banks will initiate projects concerning distributed ledger technology - the underlying technology supporting Blockchain.

1.3 How Does It Works

a. Participants and their roles

Various participants on a Blockchain network play role in its operation. Following are descriptions of each of the participants:

- **Blockchain user:** A participant (typically a business user) with permissions to join the Blockchain network, and conducts transactions with other network participants. Blockchain technology operates in the background, so the Blockchain user has no awareness of it. There are, typically, multiple users on any one business network.
- **Regulator:** A Blockchain user with special permissions to oversee the transactions happening within the network. Regulators may be prohibited from conducting transactions.
- **Blockchain developer:** Programmers who create the applications and smart contracts that enable Blockchain users to conduct transactions on the Blockchain network. Applications serve as a conduit between users and the Blockchain.
- **Blockchain network operator:** Individuals who have special permissions and authority to define, create, manage, and monitor the Blockchain network. Each business on a Blockchain network has a Blockchain network operator.
- **Certificate authority:** An individual who issues and manages the different types of certificates required to run a permissioned Blockchain. For example, certificates may be required to be issued to Blockchain users or to individual transactions.

b. Key Concepts

Four elements characterize Blockchain



To further understand how a Blockchain for business works, and to appreciate its potential for revolutionizing business networks, following are key concepts of Blockchain:

i. Shared Ledger

Ledgers are nothing new; they have been used in double-entry bookkeeping since the 13th century. What is new is the concept of a shared, distributed ledger - an immutable record of all transactions on the network, a record that all network participants can access. With a shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.

Shared ledger has the following characteristics:

- Records all transactions across the business network; shared ledger is the system of record, the single source of truth;
- Ledger is shared among all participants in the network; through replication, each participant has a duplicate copy of the ledger;
- Ledger is permissioned, so participants can see only those transactions that they are authorized to view. Participants have identities that link them to transactions, but they can choose the transaction information that other participants are authorized to view.

ii. Permissions

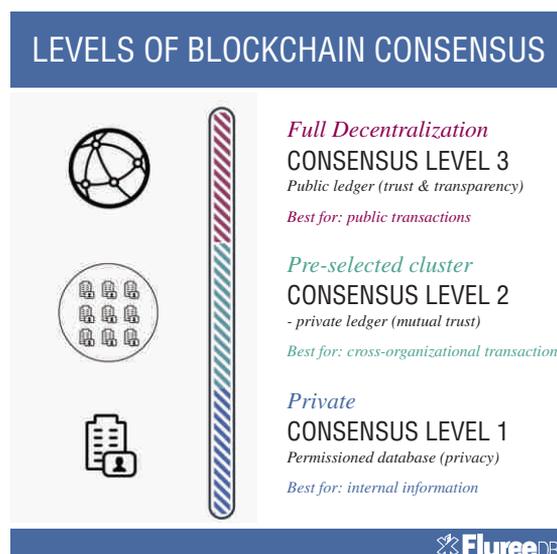
Blockchains can be permissioned or permission-less. With a permissioned Blockchain, each participant has a unique identity, which enables the use of policies to constrain network participation and access to transaction details. With the ability to constrain network participation, organizations can more easily comply with data protection regulations. Permissioned Blockchains are also more effective at controlling the consistency of the data that gets appended to the Blockchain.

With the ability to restrict access to transaction details, more transaction details can be stored in the Blockchain, and participants can specify the transaction information they are willing to allow others to view. In addition, some participants may be authorized to view only certain transactions, while others, such as auditors, may be given access to a broader range of transactions. (In a public Blockchain, the level of transaction details may be limited to protect confidentiality and anonymity.)

For example, if Party A transfers an asset to Party B, both Party A and Party B can see the details of the transaction. Party C can see that A and B have transacted but cannot see the details of the asset transfer. If an auditor or regulator joins the network, privacy services can ensure that they are able to see full details of all transactions on the network. Cryptographic technology by using digital certificates makes this possible.

Just like a passport, a digital certificate provides identifying information, is forgery resistant, and can be verified because it was issued by a trusted agency. Blockchain network will include a certification authority who issues the digital certificate.

iii. Consensus



In a network where participants are known and trusted, transactions can be verified and committed to the ledger through various means of consensus (agreement), including the following:

- **Proof of Work:** Proof of Work is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. It adds artificial computational difficulty to the ledger. The algorithm rewards miners who solve mathematical problems with the goal of validating transactions and creating new blocks.
- **Proof of Stake:** To validate transactions, validators must hold a certain percentage of the network's total value. Proof-of-stake might provide increased protection from a malicious attack on the network by reducing incentives for attack and making it very expensive to execute attacks. The creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake. There is no block reward, so, the miners take the transaction fees. Miners are also called forgers.

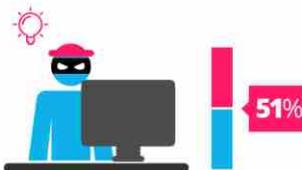
Proof of Work vs *Proof of Stake*



proof of work is a requirement to define an expensive computer calculation, also called mining



Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.



A reward is given to the first miner who solves each blocks problem.



The PoS system there is no block reward, so, the miners take the transaction fees.



Network miners compete to be the first to find a solution for the mathematical problem



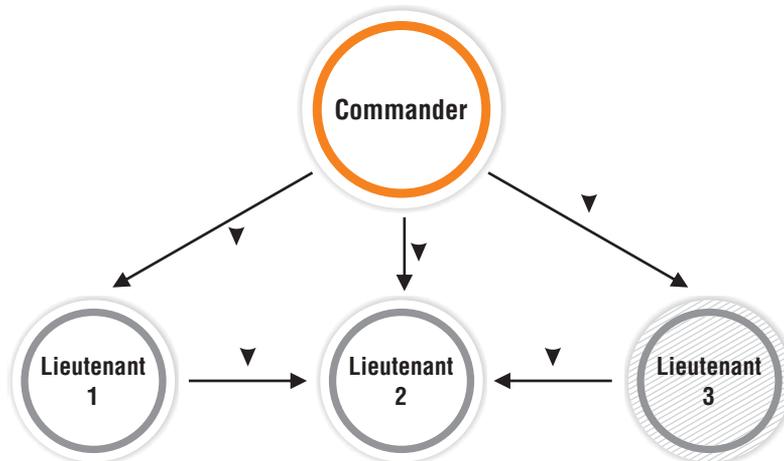
Proof of Stake currencies can be several thousand times more cost effective.

- **Multi-signature:** Majority of validators (for example, three out of five) must agree that a transaction is valid.
- **Practical Byzantine Fault Tolerance (PBFT):** An algorithm designed to settle disputes among computing nodes (network participants) when one node in a set of nodes generates different output from the others in the set.

Byzantine Generals Problems. A commanding general must send an order to his $n - 1$ lieutenant generals such that

IC1. All loyal lieutenants obey the same order.

IC2. If the commanding general is loyal, then every loyal lieutenant obeys the order he sends.



Bitcoin users protect themselves from this problem by waiting for confirmations when receiving information or payments on the Blockchain, the transactions become more irreversible as the number of confirmations increases.

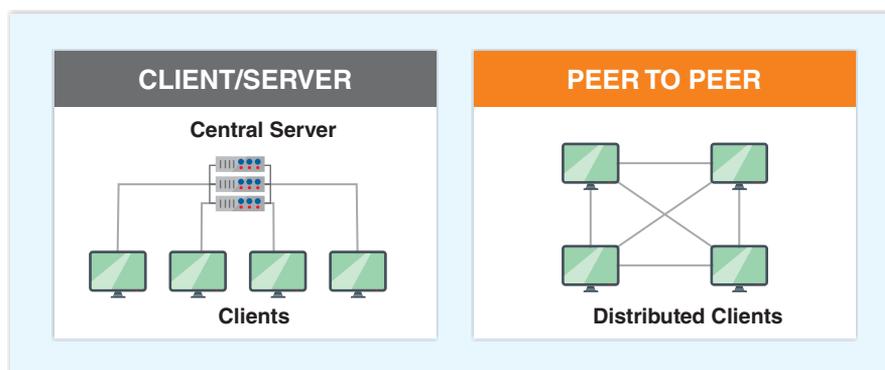
Blockchain for business features pluggable consensus, a way to implement whichever consensus mechanism is deemed best for any given industry segment.

iv. Smart Contracts

A smart contract is an agreement or set of rules that govern a business transaction; it is stored on the Blockchain and is executed automatically as part of a transaction. Smart contracts may have many contractual clauses that could be made partially or fully self-executing, self-enforcing or both. Their purpose is to provide security superior to traditional contract law while reducing the costs and delays associated with traditional contracts.

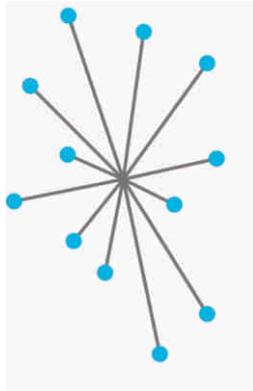
For example, a smart contract may define contractual conditions under which corporate bond transfer occurs or it may encapsulate the terms and conditions of travel insurance, which may be executed automatically when, for example, a flight is delayed by more than six hours.

v. Peer-to-peer (Distributed Network)

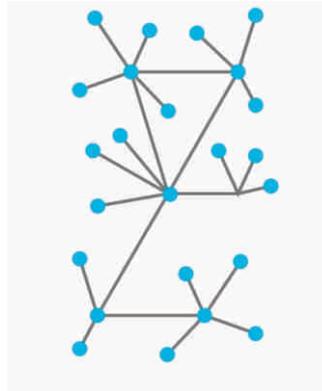


(image Source: A Gentle Introduction To Blockchain By Brave New Coin)

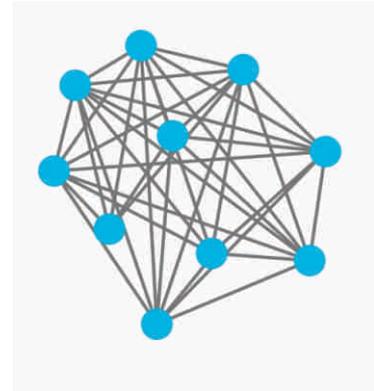
In peer-to-peer models, it's more like a gossip network where each peer has 100% of the data (or as close to it as possible), and updates are shared around. Peer-to-peer is in some ways less efficient than client-server, as data is replicated many times; once per machine and each change or addition to the data creates a lot of noisy gossip. However, each peer is more independent and can continue operating to some extent if it loses connectivity to the rest of the network. Also, peer-to-peer networks are more robust, as there is no central server that can be controlled, so closing-down peer-to-peer networks is harder.



a. Centralized



b. Decentralized



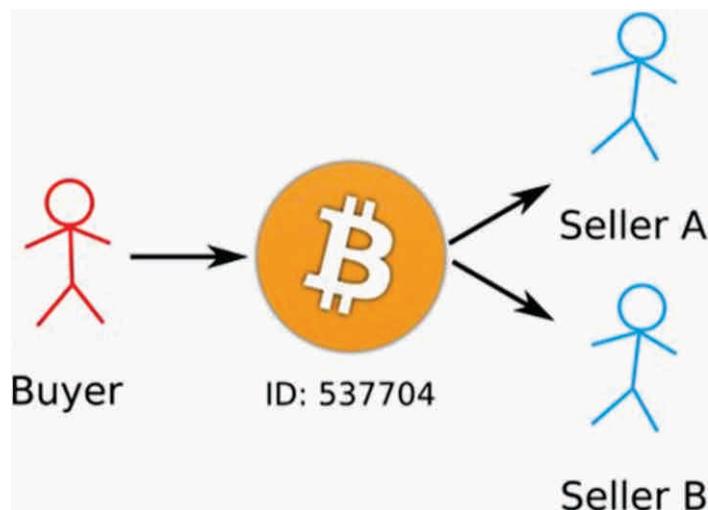
c. Distributed Network

Distributed Network

- The distributed system must ensure consistency that is when a transfer is made using the information supplied by one of the nodes it must be correctly reflected in all other nodes;
- This will either slow the things by waiting for the information to propagate across the network (known as strict consistency); or
- Slightly unreliable by confirming the transaction immediately but reserving the right to cancel it if it encounters a conflict elsewhere on the network (eventual consistency).

vi. Double Spending Problem

A risk that a digital currency can be spent twice. Double-spending is a problem unique to digital currencies because digital information can be reproduced relatively easily.

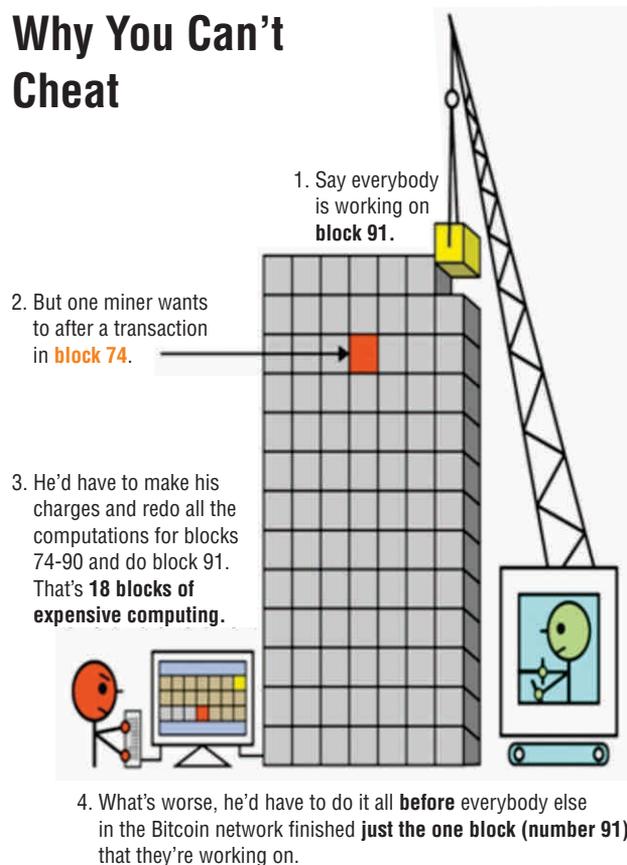


vii. Trustless

We must trust a system which we use to facilitate value exchange. When we talk about trustless systems, we mean that our ability to trust it does not depends on the intentions of any one party, which

could be arbitrarily malicious. E-mailing is a trustless system because we know that an encrypted message can be safely sent through an untrusted channel, making it a trustless system. A trustless and distributed consensus system means that if you want to send and/or receive valuable information/money from someone you do not need to trust any third-party services.

Why You Can't Cheat



Blockchain is a trust protocol, created using technology, maths and coding resulting in elimination of middlemen and addressing such concerns as:

- **Trust of Safety** - my bank is not subtracting value from my bank balance;
- **Trust of Issuance** - my bank is not printing money from nowhere;
- **Trust of correctness** - my bank ensures consistency and correctness of information.

1.4 Benefits

Global trade has been the single greatest creator of wealth in human history, and market friction the greatest obstacle to wealth. Over the years, businesses have overcome multiple sources of friction. Institutions and instruments of trust emerged to reduce risk in business transactions. Technology innovations helped overcome distances and inefficiencies. Still, many business transactions remain inefficient, expensive, and vulnerable.

Blockchain technology has the potential to remove much of the remaining market friction - the speed bumps that throttle the pace of business. As friction dissipates, a new science of organization will emerge, revolutionizing the way industries and enterprises are structured. With transparency as the norm, a robust foundation for trust can become the springboard for further ecosystem evolution. Participants and assets once shut out of markets can join in, unleashing an accelerated flow of capital and unprecedented opportunities to create wealth.

The United Nations Climate Change (UNFCCC) recently recognised the potential of blockchain to boost climate action. Its transparency, cost-effectiveness and efficiency advantages can lead to more effective stakeholder integration to take concerted actions.

Following are major perceived benefits of blockchain technology -

a. Efficiency

Blockchain technology could improve efficiency when financial entities are reconciling trades. Typically, a bank will nominate one of its systems as the golden source of trade data for any security. That golden source could be an in-house built system or an off-the-shelf solution. Reconciling this against an external party (whether that's the trading counterpart or an industry third party) has drag and inefficiencies due to system incompatibilities and processes. This leads to reconciling using the “best common technology” – typically end-of-day batch files. A Blockchain will mean that the agreed trade data is already in-house, removing the need to reconcile externally, as the Blockchain has already done that in real time.

The use of Blockchains could also help speed up payments between financial entities. As Blockchains can store data, they can also include code snippets that automate messages and one-day payments, using the “if-this-then-that” logic. If parties can agree upfront on the payoffs (usually this is agreed in term sheets written in dry legal language) and can encode the payoff terms into the trade details itself, then there will be efficiencies when trade life cycle events take place, resulting into error reduction and increase of speed. These code snippets saved onto Blockchains are called “smart contracts”.

Pure digitization of assets streamlines transfer of ownership, so transactions can be conducted at a speed more in line with the pace of doing business. Transaction time for complex, multi-party interactions are slashed from days to minutes. Transaction settlement is faster, because it does not require verification by a central authority.

b. Cost Effective

A transaction system which has been built using blockchain eliminates third party intermediaries and overhead costs for exchanging assets. A Blockchain network reduces expenses in several ways:

- Less oversight is needed because the network is self-policed by network participants, all of whom are known on the network.
- Intermediaries are reduced because participants can exchange items of value directly.
- Duplication of effort is eliminated because all participants have access to the shared ledger.

c. Enhanced Privacy

Using IDs and permissions, users can specify which transaction details they want other participants to be permitted to view. Permissions can be expanded for special users, such as auditors, who may need access to more transaction details.

d. Transparency

With trade data published to a common platform, regulators or other interested parties can plug into this and get a real time view of the trades. This gives regulators oversight into one common source, rather than receiving reports in different formats at different times from each institution. The transparency offered by Blockchains could help regulators detect systemic risks sooner.

Traditionally for trade payoffs, entities had to rely on heavy legal documentation, such as International Swaps and Derivatives Association (ISDA) master agreements. But computer code, by its very nature, is far more readable and predictable than legal language. By writing payoff structures onto a common platform in computer code which can be tested against a smart contract on a Blockchain provides for much higher levels of transparency over outcomes.

Non-financial parties could also stand to benefit from the transparency offered by Blockchain applications as they allow multiple parties to have access to the same data, where traditionally, data held by third parties can be obfuscated or withheld.

e. Governance and Trust

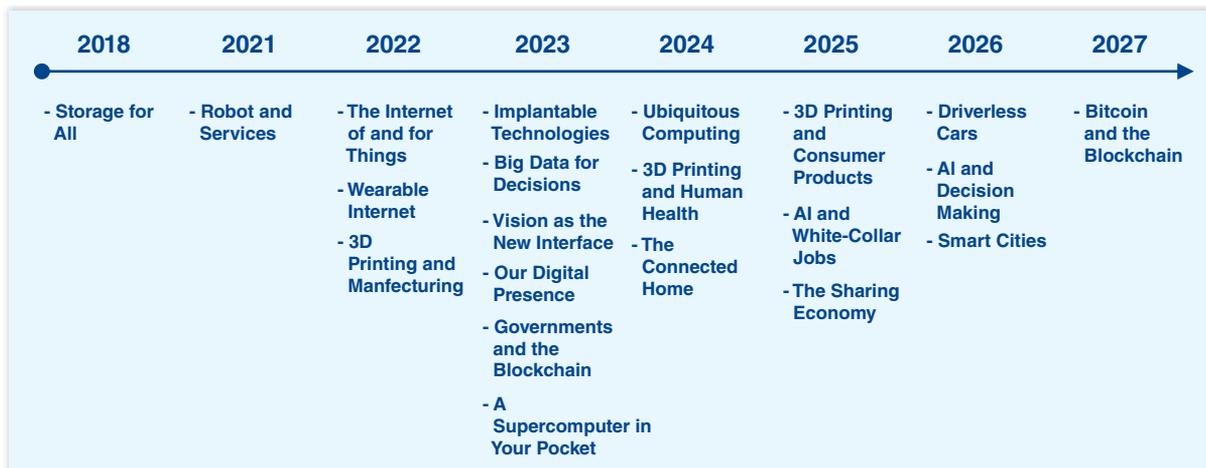
In a Blockchain system, majority of participants need to agree on data being added before it becomes part of the definitive Blockchain. This is very different to central, often secretive ledgers held and controlled centrally. When multiple parties have a say over what data is written, the ability to alter data, or remove dubious data then it creates a more honest system.

This can be explained with the help of an example like, land registry systems. In case of centrally held database, an administrator can easily make a change to records and cover their tracks without others knowing. If a land registry was recorded on a Blockchain system with multiple participants (for example, local government, regional government, perhaps other government branches and even NGOs), then prerequisite would be that the other parties would need to agree to make a change to a record. Further, any questionable changes would immediately be detected and not added without a majority consensus.

Chapter 2

WHY BLOCKCHAIN IS A DISRUPTIVE TECHNOLOGY?

2.1 Personal computers in 1975, Internet in 1993 and Digital Currency (Bitcoin, etc) in 2014 proved to be disruptive technologies. Blockchain is a foundational technology with massive potential. Blockchain is a disruptive technology because of its ability to digitize, decentralize, secure and incentivize the validation of transactions.



Blockchain provides new way of managing trust and makes organisations transparent and decentralised. It will disrupt:

- How we vote - convenient and secure voting from our smart phone, tablet, or computer and by providing voters with the ability to confirm that their vote was counted.
- How we do financial transactions - because of digital currency like, Bitcoin, blockchain will form the basis of next generation financial services infrastructure.
- How we use music - supporting a budding artist in her music career in the beginning and later reap the benefits of increased token value when she has a number one hit.
- How we claim ownership - Financial records secure money, real estate records secure property, citizen records secure credit and identities. With Blockchain, there will be undisputable proof and records of ownership.
- How we fight counterfeits - Verification of counterfeit products, diverted goods, stolen merchandise, and fraudulent transactions can be done. Some of the best use cases the solution will target include pharmaceuticals, luxury items, diamonds, and electronics. For example, using an electronic, inter-operable system organisations can identify, track and trace prescription drugs as they are distributed in the markets.

2.2 Risks for Adoption of Blockchain Technology

Blockchain adoption are not without their hurdles. Most value would come from Blockchain Technology that can share data over national borders, however, this is also the hardest to achieve without substantial political will and collaborative effort from all parties involved.

The demand for change here will come either from the grassroots demanding that certain data go on Blockchain and form a record which cannot be subsequently edited, or from regulators and policymakers mandating such

change. Having said that, Blockchain are not just about transparency and it can also be used in industry platforms for sharing of data that is helpful to the industry as a whole. In this case, a majority of players in an industry need to come together and agree on what such a platform would look like, who would pay for it, and what value each participant would get from it.

Switching technologies also cost money and cost benefit analyses need to be conducted. Blockchain solutions will need to have a clear business case before being adopted outside of pet projects.

Blockchain is a promising breakthrough technology using radical innovations. As it happens with adoption with radical innovations, there are significant risks of adoption.

- **Behaviour change:** Change is constant, but there is resistance to change. In the world of a non-tangible trusted third party, that Blockchain presents, customers need to get used to the fact that their electronic transactions are safe, secured and complete. The present-day intermediaries like, Visa or MasterCard (in case of a credit cards) will also go through change roles and responsibility.
- **Scaling:** Scaling of the current nascent services based on Blockchain presents a challenge. Executing a Blockchain transaction for the first time will require downloading the entire set of existing Blockchains and validating before executing first transaction.
- **Bootstrapping:** Moving the existing contracts or business documents/frameworks to the new Blockchain based methodology presents a significant set of migration tasks that need to be executed. For example, in case of real estate ownerships/liens, the existing documents lying in County or Escrow companies need to be migrated to the equivalent Blockchain form, which would involve time and cost.
- **Government Regulations:** In the new world of Blockchain-based transactions, Government agencies may slow down the adoption by introducing new laws to monitor and regulate the industry for compliance. In USA, this may in a way help adoption as these agencies carry customer trust. In more controlled economies like in China, the adoption will face significant headwind.
- **Fraudulent Activities:** Given the pseudonymous nature of Blockchain transactions, coupled with ease of moving valuables, there may be instances of misuse for fraudulent activities like, money trafficking. However, with enough regulations and technology support, law enforcement agencies will be able to monitor and prosecute the fraudsters.
- **Quantum Computing:** The basis of Blockchain technology relies on the very fact that it is mathematically impossible for a single party to game the system due to lack of needed computing power. With the advent of Quantum Computers (in future), the cryptographic keys may be easy enough to crack through sheer brute force approach within a reasonable time.

This will bring the whole system to its knee. The counter-argument would be for keys to become even stronger so that they may not be easy to crack.

World Economic Forum in the document “The Future of Financial Infrastructure - An Ambitious Look At How Blockchain Can Reshape Financial Services” states that additional research remains to assess distributed ledger technology feasibility, quantify benefits and analyse implementation details. Important questions to be answered moving forward :

- Cost-benefit analyses need to be conducted to determine the financial viability of distributed ledger technology
- Roadmaps need to be developed to achieve market participation/collaboration and establish standards

- Governance models, backed by societal-level discussions, need to be envisioned to support technology accountability
- Regulatory, legal and jurisdictional-specific tax frameworks need to be established and well understood.

2.3 Building Trust with Blockchain

Blockchain enhances trust across a business network. Blockchain is particularly valuable at increasing the level of trust among network participants.

Where third-party oversight is required, Blockchain reduces the burden on the regulatory system by making it easier for auditors and regulators to review relevant transaction details and verify compliance. Blockchain builds trust through the following five attributes:

- **Distributed and sustainable:** The ledger is shared, updated with every transaction, and selectively replicated among participants in near real time. Since it is not owned or controlled by any single organization, Blockchain platform's continued existence is not dependent on any individual entity.
- **Secure, private, and indelible:** Permissions and cryptography prevent unauthorized access to the network and ensure that participants are who they claim to be. Privacy is maintained through cryptographic techniques and/or data partitioning techniques to give participants selective visibility into the ledger; both transactions and the identity of transacting parties can be masked. After conditions are agreed to, participants can not tamper with a record of the transaction; errors can be reversed only with new transactions.
- **Transparent and auditable:** Since participants in a transaction have access to the same records, they can validate transactions and verify identities or ownership without the need for third-party intermediaries. Transactions are time-stamped and can be verified in near real time.
- **Consensus-based and transactional:** All relevant network participants must agree that a transaction is valid. This is achieved using consensus algorithms. Each Blockchain network can establish the conditions under which a transaction or asset exchange can occur.
- **Orchestrated and flexible:** In view of the fact that business rules and smart contracts (that are executed based on one or more conditions) can be built into the platform, Blockchain business networks can evolve as they mature to support end-to-end business processes and a wide range of activities.

Chapter 3

CURRENT USAGE OF BLOCKCHAIN

3.1 Financial Applications

Businesses need to purchase goods and services on credit with end-to-end visibility to avoid and resolve transaction disputes. For example, a company XYZ provides financing to its global partners, which enables them to purchase goods and services from suppliers with credit approved by XYZ. With over 4,000 partners and suppliers all using different and often incompatible systems, XYZ moved all the information to the Blockchain and presented it to users as a distributed ledger.

Businesses need a way to streamline the process of obtaining approvals from multiple legal entities (customs, port authorities, trucking or rail transportation firms, and so on) for the movement of goods across borders. Blockchain can be used by the legal entities to sign all approvals, and it keeps all parties informed regarding the approval status, when goods are received, and when payment is transferred from the importers to the exporter's bank.

Banks need a way to manage nostro/vostro accounts. Nostro (ours) refers to an account a domestic bank holds in a foreign bank in the foreign country's currency. Vostro (yours) is how the foreign bank refers to that account. Such accounts are used to facilitate and simplify trade and foreign exchange transactions through reconciliation. Nostro/vostro accounts can become stored account transactions on a Blockchain to dramatically improve transparency and efficiency through automated reconciliation of accounts.

a. Private Securities

It is very expensive to take a company public. A syndicate of banks must work to underwrite the deal and attract investors. The stock exchanges list company shares for secondary market to function securely with trades settling and clearing in a timely manner. It is now theoretically possible for companies to directly issue the shares via the Blockchain. These shares can then be purchased and sold in a secondary market that sits on top of the Blockchain. Here are some examples:

- **NASDAQ Private Equity:** NASDAQ has launched its Private Equity Exchange in 2014. This is meant to provide the key functionalities like, Cap table and investor relationship management for the pre-IPO or private companies. The current process of trading stocks in this exchange is inefficient and slow due to involvement of multiple third parties. NASDAQ has joined hands with a Start-up called chain.com to implement private equity exchange on top of Blockchain. Chain.com is implementing Blockchain based smart contracts to implement exchange functionality. This product is expected to be fast, traceable and efficient.
- **Medici** is being developed as a securities exchange that uses the Counterparty implementations of Bitcoin 2.0. The goal here is to create a cutting-edge stock market. Counterparty is a protocol that implements traditional financial instruments as the self-executing smart contracts. These smart contracts facilitate, verify or enforce the negotiation of contract and eliminate the need for a physical document. This eliminates the need for an intermediary, such as, broker, exchange or bank.
- **Blockstream** is an open source project with focus on sidechains-interoperable Blockchains - to avoid fragmentation, security and other issues related to alternative crypto-currencies. Uses can range from

registering securities, such as stocks, bonds and derivatives, to securing bank balances and mortgages.

- Coin setter is a New York based bitcoin exchange. It is working on a Project Highline, a method of using the Blockchain to settle and clear financial transactions in T+ 10 minutes rather than the customary T+3 or T+2 days.
- Augur is a decentralized prediction market that will allow users to buy and sell shares in anticipation of an event with the probability that a specific outcome will occur. This can also be used to make financial and economic forecasts based on the “wisdom of crowds”.
- Bitshares are digital tokens that reside in the Blockchain, with reference to specific assets such as, currencies or commodities. Token holders may have the unique feature of earning interest on commodities, such as gold, and oil, as well as dollars, euros and currency instruments.

b. Insurance

Insurance industry can also use Blockchain. Insurance providers need an efficient way to process claims, verify that an insurable event (such as an accident) actually occurred, and provide customers with fair and timely pay-outs.

With automated insurance claim processing, policy conditions are written into a smart contract stored on the Blockchain and connected to publicly available data via the Internet. In such a case, whenever an insurable event occurs and is reported by a trusted source, insurance policy is automatically triggered, claim is processed according to the terms of the policy specified in the smart contract, and the customer is paid.

Assets which can be uniquely identified by one or more identifiers, which are difficult to destroy, or replicate can be registered in Blockchain. This can be used to verify ownership of an asset and trace the transaction history. Any property (physical or digital such as real estate, automobiles, physical assets, laptops, other valuables) can potentially be registered in Blockchain and the ownership, transaction history can be validated by anyone, especially insurers.

Benefits for insurance are as follows:

- Eliminates the cost of processing insurance claims;
- Reduces the opportunity for insurance fraud;
- Improves customer satisfaction.

For example, Ever ledger is a company which creates permanent ledger of diamond certification and the transaction history of the diamond using Blockchain. The characteristics which uniquely identify the diamond such as, height, width, weight, depth, colour, etc., are hashed and registered in the ledger. Verification of diamonds can be done by insurance companies, law enforcement agencies, owners and claimants. Ever ledger provides a simple to use web service API for looking at a diamond, create/read/update claims (by insurance companies) and create/read/update police reports on diamonds.

c. Government

A considerable amount of government machinery is involved in recording transactions and tracking ownership of assets, all of which can be made more efficient and transparent using Blockchain. Establishing trusted identity remains a problem due to forgery and expensive background checks required in verification. Millions upon millions of refugees and their children go undocumented. People in the poorer parts of the world may not have sufficient proof to establish identity as required by certain service providers; for example,

banks typically require proof of residence or utility bills to establish identity, neither of which may exist in the under developed countries. Organizations can apply Blockchain by issuing digitally authenticated birth certificates that are unforgeable, time-stamped, and accessible to anyone in the world.

INDIA FUTURE USE CASE - A CORE BHARATCHAIN NETWORK (CBCN)

On a Blockchain fabric, the entire network should be on a single fabric type - rather than each government body or department developing its own. This way, Blockchain network can fulfil multiple use cases that span Central as well as State Governments, aiding interoperability in terms of data flow and communications.

SIDENCHAINS

BharatChain can comprise multiple Blockchains, each holding data that may be needed across the other Blockchains. To enable sharing of this data, rather than creating a centralized database, where Blockchains can write and read data as required, Sidechains are a better option.

NODES

Government Blockchain should be a permissioned system. For example, select set of Government agencies will have 'transaction initiation', 'read' and 'validation' rights whereas certain other participants like schools, hospitals and other businesses will have 'transaction initiation' and 'read' rights only. Further, third party auditors may be limited to having just 'read/querying' rights. Probable benefits are reduced costs and time in identity verification, reduction in human trafficking and transparency in grant allocations.

d. Automotive

For tracking vehicle ownership with Blockchain, a robust system on following lines may be created:

- The government/regulator creates and populates the registration for the new vehicle on the Blockchain and transfers the ownership of the vehicle to the manufacturer.
- The manufacturer adds the make, model, and vehicle identification number to the vehicle template within the parameters allowed by the smart contract (a digital agreement or set of rules that govern a transaction).
- The dealer can see the new stock availability, and ownership of the vehicle can be transferred from the manufacturer to the dealership after a smart contract is executed to validate the sale.
- The leasing company can see the dealer's inventory. Ownership of the vehicle can be transferred from the dealer to the leasing company after a smart contract is executed to validate the transfer.
- The lessee can see the cars available for lease and complete required form to execute lease agreement.
- The leasing process continues between various lessees and the leasing company until the leasing company is ready to retire the vehicle. At this point, ownership of the asset is transferred to the government authorised scrap merchant, who, according to another smart contract, has permission to dispose of the vehicle.

e. Manufacturing

In the case of manufacturing sector, the best use case is ensuring contracts are executed and ensuring payment of credits.

- Applications can be used to track credit cycle payments, design stock movements and make purchase decisions.
- Blockchain system ensures design department communicates its plans to the entire chain and only if the chain accepts the viability then only the business will move forward with execution.
- Product Planning department could get in to its own distributed ledger and integrate its vendors on to the

Blockchain platform, so the “bill-of-materials” is executed with precision. There cannot be additional items billed and neither will there be graft in over invoicing.

- Marketing team can have a Blockchain system for its dealers to track all orders and contracts on the chain.
- At the board level, these transactions are observed on a real-time basis.
- This will boost the sharing economy and the world will not need assets that are unproductive because it has all the necessary parties aligned in a single chain.

f. Banking

- Blockchain can be useful in credit functions like, letter of credit. Till recently, all communication between Buyer, Issuing Bank, Seller and Seller's Bank was on paper, e-mail and phone calls. New technologies will make banks work faster with their customers and ensure transparency at all levels.
- Blockchain will cut out duplication in a multi-party system like, asset financing and EMI payments.

3.2 Non-Financial Applications

a. Supply Chain Management

When something goes wrong with a complex “system of systems”, such as an aircraft, it is important to know the provenance, through supply chain management, of each component, down to the manufacturer, production date, batch, and even the manufacturing machine program. Blockchain holds complete provenance details of each component part, accessible by each manufacturer in the production process, like, aircraft owners, maintainers, and government regulators. Benefits in this category include:

- Increased trust because no single authority “owns” the provenance information;
- Increased efficiencies lead to reductions in time taken to diagnose and remedy a fault improving system utilization;
- Specific recalls rather than cross fleet/generic.

b. Healthcare

Healthcare industry needs a more efficient and secure system for managing medical records, pre-authorizing payments, settling insurance claims, and performing and recording other complex transactions. Blockchain promises to provide much needed relief. Electronic medical records are currently maintained in data centres (in a cloud-like environment) and access is limited to hospital and care provider networks. Centralization of such information makes it vulnerable to security breach and can be expensive. In such a case, Blockchain can be used to hold the complete medical history for each patient, with multiple granularities of control by the patient, doctors, regulators, hospitals, insurers, and so on, providing a secure mechanism to record and maintain a comprehensive medical history for every patient.

Under a Blockchain network, every citizen who is insured can use government-provided or private insurance in any hospital and not be denied service. Aadhaar number can be linked to verify the individual, and the system will generate blocks of transactions that insurance companies and hospitals must honour provided the information of the citizen is correct. If the information is wrong, the ledger identifies that the process need not be executed and, therefore, all parties agree not to execute the transaction. Blockchain will make sure that every transaction with the hospital is tracked and makes sure that the patient is screened faster. For example, DOTS program in India with WHO for TB eradication.

Following benefits are realized:

- Tamper-resistant means of storing medical history;
- Reduced time in resolution of insurance claims and increased efficiency in providing insurance quotes;

- Complete medical history of the patient for use by physicians for precise drug recommendations.

Healthcare payments pre-authorization - The term “clinical attachments” is a concept surrounding the need for additional clinical information when a payer is adjudicating a healthcare claim. Claims are often submitted without all the required supporting details, so payer(s) need to request additional detail, which adds costs and delays to the settlement process. Further, matching up the claims with the supporting information is challenging for all parties involved. Blockchain can simplify this complicated and time-consuming process and automate the collection and sharing of information.

Additional benefits including claims can be reviewed and paid more efficiently and quickly; and the system can suggest alternative services that have better coverage.

c. Global Logistics and Shipping

As machines interact with one another, any relevant interactions can be reported by the machines and recorded in the Blockchain to increase efficiency and accuracy and reduce costs. Trade logistics use case applies Blockchain to automate IoT (Internet of Thing) processes. Currently, freight logistics involve many different parties like, manufacturers, forwarders, shippers, custom agents, and insurers.

Although parties often interact and depend on one another, they may have different goals and use different systems to track shipments. An IoT-enabled Blockchain is used as a shared ledger to record shipping containers as they move through system. Smart contracts can be automatically updated through the IoT foundation and can be optimized to exploit IoT-enabled international trade on Blockchain.

Following benefits can be realized:

- Greater transparency of shipment progress improves efficiency;
- Trust grows, as all transactions are indelibly recorded;
- Accuracy is improved, and costs are cut through IoT participation;
- Participants gain the ability to optimize and automate business processes through IoT;
- Future vision allows for “freight autonomy”.

d. Notary Public and Deed Records

Verification of authenticity of any document can be done using Blockchain and eliminates the need for centralized authority. The document certification service helps in Proof of Ownership (who authored it), Proof of Existence (at a certain time) and Proof of Integrity (not tampered) of documents. Since it is counterfeit-proof and can be verified by independent third parties so these services are legally binding. Using Blockchain for notarization secures the privacy of the document for those who seek certification. By publishing proof of publication using cryptographic hashes of files into Blockchain would take the notary time stamping to a new level. It would thereby also eliminate the need for expensive notarization fees and ineffective ways of transferring documents.

For example, Stampery is a company which can stamp e-mails or any files using Blockchain. It simplifies certifying of e-mails by just e-mailing them to an e-mail specifically created for each customer. Law firms are using Stampery’s technology as it is a very cost-effective way to certify documents. Viacoin is the one of the companies which uses clearinghouse protocol for notary services. Block Notary is an iOS app which helps to create proof of existence of any content (photo, files, any media) using TestNet3 or Bitcoin network. Crypto Public Notary uses Blockchain of Bitcoin to notarize documents by using trivial number of bitcoins to

record the file's checksum in public Blockchain. Ascribe is another company which does authorship certification using Blockchain. It also offers transfer of ownership service with attribution to the original author.

e. Music Industry

Music industry has gone a big change in the last decade due to the growth of Internet and availability of several streaming services over the Internet. It is impacting everyone in the music industry including artists, labels, publishers, songwriters and streaming service providers. The process by which music royalties are determined has always been convoluted one, but the rise of the Internet has made it even more complex giving rise to the demand of transparency in the royalty payments by artists and songwriters.

This is where the Blockchain can play a significant role by maintaining a comprehensive, accurate distributed database of music rights ownership information in a public ledger. In addition to rights ownership information, royalty split for each work, as determined by “smart contracts” could be added to the database. Smart contracts would define relationships between different stakeholders (addresses) and automate their interactions.

f. Decentralized Proof of Existence

Validating the existence or the possession of signed documents is very important in any legal solution. Traditional document validation models rely on central authorities for storing and validating the documents, which present some obvious security challenges. These models become even more difficult as the documents become older.

Blockchain technology provides an alternative model to proof-of-existence and possession of legal documents. By leveraging Blockchain, a user can simply store the signature and timestamp associated with a legal document in the Blockchain, and can validate it anytime using native Blockchain mechanisms.

Proof of Existence is a simple service that allows one to anonymously and securely store online proof of existence of any document. This service simply stores the cryptographic digest of the file, linked to the time in which a user submits his/her document. It is to be noted here that cryptographic digest or fingerprint(not the actual document) is stored in Blockchain, so user need not be worried about the privacy aspect. This, therefore, allows a user to later certify the existence of a document that existed at a certain time.

Major advantages of this service are security and privacy that allows a user to give decentralized proof of the document that cannot be modified by a third party. Existence of the document is validated using Blockchain that does not depends on a single centralized entity.

g. Decentralized Storage

Cloud file storage solutions such as, Dropbox, Google Drive or One Drive are growing in popularity to store documents, photos, video and music files. Despite their popularity, cloud file storage solutions typically face challenges in areas such as, security, privacy and data control. Major issue is that one must trust a third party with one's confidential files.

Some organisations are providing Blockchain based peer-to-peer distributed cloud storage platform that allows users to transfer and share data without relying on a third-party data provider. This allows people to share unused internet bandwidth and spare disk space in their personal computing devices to those looking

to store large files in return for bitcoin-based micro payments.

Absence of a central control eliminates most traditional data failures and outages, as well as significantly increases security, privacy and data controls. For example, Storj platform depends upon a challenge algorithm to offer incentivization for users to properly participate in this network. In this way, Storj platform can periodically cryptographically check the integrity and availability of a file and offer direct rewards to those maintaining the file. Here, bitcoin-based micro payments serve as both an incentive and payment, while a separate Blockchain is used as a data store for filing metadata.

h. Decentralized IoT

Internet of Things (IoT) is increasingly becoming popular technology in both the consumer and the enterprise space. A vast majority of IoT platforms are based on a centralized model in which a broker or hub controls the interaction between devices, however, this approach has become impractical for many scenarios in which devices need to exchange data between themselves autonomously. This specific requirement has led to efforts towards decentralized IoT platforms.

Blockchain technology facilitates the implementation of decentralized IoT platforms such as, secured and trusted data exchange as well as record keeping. In such architecture, Blockchain serves as the general ledger, keeping a trusted record of all the messages exchanged between smart devices in a decentralized IoT topology.

For example, IBM in partnership with Samsung has developed a platform ADEPT (Autonomous Decentralized Peer to Peer Telemetry) that uses elements of the bitcoin's underlying design to build a distributed network of devices for example, a decentralized Internet of Things (IOT). ADEPT uses three protocols-BitTorrent (file sharing), Ethereum (Smart Contracts) and TeleHash (Peer-To-Peer Messaging)-in the platform. Filament is a start-up that recently announced a new chip designed to enable industrial IoT devices to work with multiple blockchain technologies.

i. Anti-Counterfeit Solutions

Counterfeiting is one of the biggest challenges in the modern commerce. It is one of the biggest challenge that digital commerce world faces today. Existing solutions are based on reliance and trust on a third party trusted entity that introduces a logical friction between merchants and consumers.

Blockchain technology with its decentralized implementation and security capabilities provides an alternative to existing anti-counterfeiting mechanisms. One can envision a scenario, in which brands, merchants and marketplaces are part of a Blockchain network with nodes storing information to validate the authenticity of the products. With the use of this technology, stakeholders in the supply chain need not rely on a centralized entity for authenticity of the branded products.

For example, Block Verify provides Blockchain based anti-counterfeit solutions that introduce transparency to supply chains. It is finding applications in pharmaceutical, luxury items, diamonds and electronics industries.

j. Internet Applications

Internet applications can be developed based on blockchain technology. For example, Namecoin is an alternative Blockchain technology (with small variations) that is used to implement decentralized version of

Domain Name Server (DNS) that is resilient to censorship. Current DNS servers are controlled by governments and large corporations, and could abuse their power to censor, hijack, or spy Internet usage. Use of Blockchain technology means since DNS or phonebook of the Internet is maintained in a decentralized manner and so every user can have the same phone book data on their computer.

Public Key Infrastructure (PKI) technology is widely used for centralized distribution and management of digital certificates. Every device needs to have root certificate of the Certification Authority (CA) to verify digital signature. While PKI have been widely deployed and incredibly successful, dependence on a CA makes scalability an issue. Characteristics of Blockchain can help address some of the limitations of the PKI by using Keyless Security Infrastructure (KSI). KSI uses cryptographic hash function, allowing verification to rely only on the security of hash functions and availability of a Blockchain.

k. Retail/E-Commerce

Stock reaching the store on time is not guaranteed as it requires co-ordination between various parties.

- Store Manager wants a variety of goods.
- Merchandise Department must ensure the factory and warehouse have the said goods in stock.
- Factory informs all three about the production schedule and availability of goods.
- Warehouse keeps in touch with Merchandise and Factory.

Blockchain can handle the communication between the four parties efficiently. Services like, AI and machine learning (ML) can be built on top of Blockchain to allow retailers to take decisions faster.

l. Others

Other Non-Financial Implications are -

- Small and Medium Enterprises (SMEs) - In India, many SMEs are at the mercy of large companies, many a times payments are delayed and credit cycles are adverse. For such SMEs, legal recourses are an expensive proposition, and here Blockchain can solve their problem as it can execute contracts because the information is secured in a ledger and cannot be tampered with.
- I own my data - Enabling individuals to own and monetize their data and protect privacy.
- Protecting Digital Assets - Ensuring IP rights and compensation to the creators of value.
- Fair Game - Free and fair voting and elections can be made possible through use of Blockchain technology.
- Easy Remittances - Affordable and effective cross-border payments and remittances.
- Immutable - Protection of rights through immutable records.
- Single Fabric - Blockchain's transformative power across various Industries needs collaborative efforts.
- Blockchain-as-a-Service (BaaS)- This will not only minimise the frauds happening in healthcare, digital payments, supply chains, banking, energy trading, public services, but the technology will also maximise the efficiency and transparency in all these correlated sectors.

Chapter 4

ACCOUNTING ASPECT OF BLOCKCHAIN

4.1 Traditional accounting practice comprises of the financial records in private ledgers and relies on accountants to reconcile them against those maintained by the third-party counterparts. This tedious and labour-intensive work brings upon higher human resource cost, lower efficiency and work load especially on the month and year ends. Blockchain alters the conventional techniques for invoicing, documentation, contracts and instalment preparation. It mechanizes these physically performed assignments.

4.2 Potential to Enhance Accounting System

Modern financial accounting is based on a double entry system. Double entry bookkeeping revolutionized the field of financial accounting during the Renaissance period; it solved the problem of managers knowing whether they could trust their own books. However, to gain the trust of outsiders, independent public auditors also verified the company's financial information.

Blockchain technology may represent the next step for accounting. Instead of keeping separate records based on transaction receipts, companies can write their transactions directly into a joint register, creating an interlocking system of enduring accounting records. Since all entries are distributed and cryptographically sealed, falsifying or destroying them to conceal activity is practically impossible. It is like the transaction being verified by a notary - only in an electronic way.

Companies would benefit in many ways: Standardisation through blockchain would allow auditors to verify a large portion of the most important data behind the financial statements automatically. The cost and time necessary to conduct an audit would decline considerably. Auditors could thereby spend more time on areas where they can add more value, e.g., on very complex transactions or on internal control mechanisms.

4.3 Skills for the Future

Following are some skills that will be required by professional accountants in future -

- Areas of accounting concerned with transactional assurance and carrying out transfer of property rights will be transformed by Blockchain and smart contract approaches.
- Reduction in the need for reconciliation and dispute management, combined with increased certainty around rights and obligations, will allow greater focus on how to account for and consider the transactions, and enable an expansion in specific areas that can be accounted for.
- Many current-day accounting department processes can be optimised through Blockchain and other modern technologies, such as data analytics or machine learning. This will increase the efficiency and value of the accounting function.
- It is perceived that spectrum of skills represented in accounting will change. Some work such as, reconciliations and provenance assurance will be reduced or eliminated, while other areas such as, technology, advisory, and other value-adding activities will expand.
- To properly audit a company with significant Blockchain-based transactions, focus of auditor will have to shift. There will be little need to confirm accuracy or existence of Blockchain transactions with external sources, but there will be plenty of attention required to be paid to how those transactions have been

recorded and recognised in the financial statements, and how judgemental elements such as, valuations have been decided.

- In the long term, more and more records could move onto Blockchains, and auditors and regulators with access would be able to check transactions in real time and with certainty over the provenance of those transactions.
- Accountants will be required to know how to advise on Blockchain adoption and consider the impact of Blockchain on their professional work. They also need to be able to act as the bridge, having informed conversations with both technologists and business stakeholders.
- Accountants' skills will need to expand to include an understanding of the principle features and functions of Blockchain.

4.4 How Accountancy Profession Can Lead in Blockchain Landscape

Move to a financial system with a significant Blockchain elements offers many opportunities for the accountancy profession. Accountants are experts in record keeping, application of complex rules, business logic and standards setting. They can guide and influence how Blockchain is embedded and used in the future, and to develop Blockchain-led solutions and services. To become truly an integral part of the financial system, Blockchain must be developed, standardised and optimised. This process is likely to take many years. There are many Blockchain applications and start-ups in this field, but there are very few that are beyond the proof of concept or pilot study stage.

Accountants are already participating in research, but there is more for the profession to contribute in establishment of new financial services infrastructure and processes in Blockchain innovation landscape. Crafting regulation and standards to cover Blockchain will be no small challenge, and leading accountancy firms and bodies can bring their expertise to that work. Accountants can also work as advisers to companies considering joining Blockchain themselves, providing advise on weighing the costs and advantages of the new system, etc. Accountants' mix of business and financial nous will position them as key advisers to companies approaching these new technologies looking for opportunity.

Chapter 5

ASSURANCE OF BLOCKCHAIN BASED SYSTEMS / PROCESSES

5.1 Impact of Blockchain on Audit/Assurance

Presently, assurance processes are resource intensive, time intensive and many a times there is lack of technology integration. World Economic Forum's document "The Future of Financial Infrastructure - An Ambitious look at How Blockchain Can Reshape Financial Services" mentions following constraints of current assurance process -

- Resource Intensive - Scope formation, risk assessment and audit planning require representatives from multiple functional areas, reducing productivity as individual employees cannot complete their daily activities;
- Time Intensive Review - Pulling sample data for audit review is time intensive and inefficient due to dependency on manual activities;
- Lack of technology integration - Information is copied from source systems and provided to auditors, adding inefficient manual processes that increases the likelihood of errors.

This document mentions future state benefits of Blockchain/Distributed Ledger Technology (DLT) as follows -

- Data transparency - Enabling data stored within financial systems to be accessible via DLT through the financial data extraction layer provides immutable and transparent records that are updated in real time;
- Automated review - Financial information accessible via DLT enables an automated review via audit software, reducing the time and resources required to perform these activities;
- Reduced errors - Audit teams have authorized access to financial data, eliminating errors generated by manual activities and streamlining the update process;
- Integrated systems - Reporting systems executed via DLT facilitates the creation of quarterly and annual filings, reducing duplicate efforts.

Blockchain technology offers an opportunity to streamline financial reporting and audit processes. Today, account reconciliations, trial balances, journal entries, sub-ledger extracts, and supporting spreadsheet files are provided to an auditor in a variety of electronic and manual formats. Each audit process begins with different information and schedules that require an auditor to invest significant time when planning an audit. In a Blockchain world, an auditor will have near real-time data access via read-only nodes on Blockchains. This may allow an auditor to obtain information required for the audit in a consistent, recurring format. As more and more entities and processes migrate to Blockchain solutions, accessing information in the Blockchain will likely to become more efficient. For example, if a significant class of transactions for an industry is recorded in a Blockchain, it might be possible for an auditor to develop software to continuously audit organizations using the Blockchain.

Further, speeding up audit preparation activities could help reduce the lag between the transaction and verification dates. Reducing lag time could offer the opportunity to increase the efficiency and effectiveness of financial reporting and auditing by enabling management and auditors to focus on riskier and more complex transactions while conducting routine auditing in near real time. With Blockchain-enabled digitization, auditors could deploy more automation, analytics and machine-learning capabilities such as, automatically alerting relevant parties about unusual transactions on a near real-time basis. Supporting documentation, such as

contracts, agreements, purchase orders, and invoices could be encrypted and securely stored or linked to a Blockchain. By giving auditors access to unalterable audit evidence, the pace of financial reporting and auditing could be improved significantly.

While the audit process may become more continuous, auditors will still have to apply professional judgment when analysing accounting estimates and other judgments made by management in the preparation of financial statements. In addition, for areas that become automated, they will also need to evaluate and test internal controls over the data integrity of all sources of relevant financial information.

5.2 Future Roles of Chartered Accountants in Blockchain Ecosystem

Following is list of potential new roles for chartered accountants in Blockchain landscape, which is illustrative only and not all-inclusive:

a. Audit of Smart Contracts

Contracting parties may want to engage an assurance provider to verify that smart contracts are implemented with the correct business logic. Professional Accountants could verify the interface between smart contracts and external data sources that trigger business events. Without an independent evaluation, users of Blockchain technologies face the risk of unidentified errors or vulnerabilities. To take on this new role, professional accountants may need a new skill set, including understanding technical programming language and Blockchain functionality.

In the context of a financial statement audit, management will be responsible for establishing controls to verify whether the smart-contract source code is consistent with the intended business logic. Professional Accountant auditing an entity with smart contracts/Blockchain is likely to consider management's controls over the smart contract code. Many companies may choose to reuse smart contracts built by other entities already active on a Blockchain. Future auditing standards and auditing guidance may need to contemplate this technology and thereby bring clarity to the role of the professional accountants in those scenarios.

b. Service Auditor of Consortium Blockchain

Prior to launching a new application on an existing Blockchain platform or leveraging/ subscribing to an existing Blockchain product, users of the system may desire independent assurance as to the stability and robustness of its architecture. Instead of each participant performing their own due diligence, it may be more efficient to assign this task to a Professional Accountant to achieve these objectives. Critical Blockchain elements (e.g., cryptographic key management) should be designed to include sophisticated General Information Technology Controls (GITCs) that provide ongoing protection for sensitive information, as well as processing controls over security, availability, processing integrity, privacy and confidentiality. On an ongoing basis, a trusted and independent third party may be needed to provide assurance as to the effectiveness of controls over a private Blockchain.

c. Central Access Granting Administrator

Permissioned Blockchain solutions may benefit from a trusted, independent and unbiased third party to perform the functions of a central access-granting administrator. This function could be responsible for verification of identity or a further vetting process to be completed by a participant before they are granted access to a Blockchain. This central administrator could validate the enforcement and monitoring of Blockchain's protocols. If this function is performed by a user/node of the Blockchain, then an undue advantage could exist and trust among consortium members could be weakened. Since this role would be designed to create trust for the Blockchain as a whole, due care will be needed when establishing both its

function and its legal responsibilities. As a trusted professional, professional accountant is capable of carrying out this responsibility.

d. Arbitration Function

Business arrangements can be complex and result in disputes between even the most well-intentioned parties. For a permissioned Blockchain, an arbitration function might be needed in the future to settle disputes among the consortium Blockchain participants. This function is analogous to the executor of an estate, a role typically filled by various qualified professionals, including professional accountants. Participants on the Blockchain may require this type of function to enforce contract terms where the spirit of the smart contract departs from a legal document, contractual agreement or letter.

Chapter 6

ADOPTION AND THE PHASES OF DEVELOPMENT

6.1 Phase I: Early Adoption by Accounting Firms

Accounting firms have already started research on Blockchain -

- Platforms are being created to simplify and speed up the auditing process of Blockchain transactions.
- Prototypes and pilot projects in digital identity, trade, international transactions, banking, management of loyalty and rewards programs are being created.
- Differentiated approach on editable Blockchains is being adopted.
- Digital Ledger Services are being introduced to improve transactional speed and security, cut costs and digitise back-office operations.
- Accounting firms are acknowledging disruptive nature of Blockchain and are exploring various applications of this nascent technology. They are piloting public, private and permissioned Blockchain technologies to better adapt to client needs.
- They are gravitating away from Bitcoin-Blockchain association and moving to the capabilities of private and permissioned ledgers.
- These pilot projects, partnerships and alliances reflect the growing impact Blockchain is already having on the accounting industry.

6.2 Phase II: Approaching Mainstream Adoption (critical mass in 3.5 years)

Following are important aspects in Phase II, i.e., approaching mainstream adoption -

a. Streamlining internal accounting practices and processes

Employing Blockchain will certainly improve client services but far greater use of this technology is in internal accounting management. Blockchain can remove Rube Goldberg processes (complicated tools/processes doing simple jobs) specifically in the areas of tax and assurance. Blockchain would become a congruent and perfectly matched record of transactions ensuring integrity and transparency for everyone involved.

b. Real-time Audit trail and Assurance

Entries recorded in real-time on Blockchain platforms are especially important for assurance providers, advisors and organizational stakeholders. Overall risk of making incorrect entries is significantly reduced because the transactions are logged by both parties, time-stamped, and verified via decentralization (in case of public Blockchain).

Being able to track historical data with such accuracy and efficiency helps to paint a clearer picture of a company's financial standing and overall performance. Real-time entries can also help draw attention to hidden accounts and minute details that may have otherwise been overlooked. Professional accountants can convert these up-to-date figures into useful information for management regarding wasted resources, redundant practices, and bottleneck processes that might be hindering performance. The real-time element of Blockchain allows professional accountants to focus on this kind of value-added work by significantly reducing the time needed to verify a company's accounting entries. With Blockchain, the scope of auditing drastically increases since the audit trail becomes more aggregated and accessible to accountants and other regulators. As such, this will improve auditors' chances of uncovering fraudulent activity.

c. Smart Contracts, Supply chain management and Real-time analytics

Self-executing, programmed code within the Ethereum Blockchain acts in response to a set of conditions is not limited to legal and managerial implications but it can replace virtually any tasks that can be automated, including administrative, operational and performance reviewing functions. Smart contracts could be set up to automatically transfer funds/assets based on commands inputted by users of the software or conditions stipulated in receipts, royalty contracts, and payment schedules.

Interest payments could also be managed more effectively using smart contracts and additional ledger accounts. Capital asset accounts could integrate smart contracts to regularly depreciate equipment in order to keep the net book value up-to-date. Most well-known trailblazer for supply chain management using Blockchain technology is Provenance. Status of raw materials, work-in-process, and finished goods becomes more traceable, more accurate, and less time consuming for the professional accountant to consolidate. Smart contracts, supply chain management and real-time analytics work in unison to automate parts of the monthly consolidation process for sustainability and financial reporting.

d. Taxation and Revenue Recognition

Using current accounting principles, revenue recognition and tax allocation are done retrospectively. However, Blockchain technology has the potential to record each of those instantaneously in real-time. This in turn would make tax evasion virtually impossible and lower the cost of tax compliance. UK Government Advisors have proposed that Blockchain technology be integrated to automatically calculate value-added taxes (VAT)/goods and services taxes (GST).

Coupling the real-time features of Blockchain with smart contracts to ensure Anti-Money Laundering (AML) compliance would also make organisations less likely to engage in illicit tax practices. There would be more transparency, making it easier for regulators to expose companies engaging in tax fraud.

Since third party records would now be digitized in real-time, firms would not have to wait for their transactions to be cleared or balanced by an intermediary. Additional ledgers can also be set up to track repair and maintenance expenditures to capital assets, which can be cited in insurance clauses. Likewise, accounts receivable/payable, intangible assets, inventory accounts, and long-term and short-term loans will also be redefined by Blockchain.

e. Cost Saving

Tax compliance costs would be significantly reduced because taxation process could be automated via Blockchain. Using Blockchains for distributed storage and processing (rather than relying on centralized databases) can be 90 to 95% cheaper. In its 2016 report, Goldman Sachs also projected that up to \$90 million can be saved from cost reductions and \$700 million from IT improvements.

An argument could be that these examples suffer from a cherry-picking fallacy or a hasty generalization and that these cost savings will be counteracted by initial (and ongoing) investments in new Blockchain infrastructure. However, it is important to remember that every firm and every industry is unique. There are many factors to be considered before implementation including the size of the firm, the nature of the business, the competitive environment, choosing between internal development or BaaS, and the capital resources available.

In any case, professional accountants will need to acquire new skills and hone existing competencies in order to adapt to the industry's dynamic and rapidly changing technological landscape. These features allow

professional accountants to free up more time to interpret information and provide consultations to clients for decision-making.

6.3 Phase III - Global Adoption (Maturity by 2025)

Blockchain technology has the potential to completely reshape capital markets. At its early stages, Blockchain will be able to streamline accounting through triple-entries and smart contracts. In finance, it can make transferring financial instruments much more efficient. However, in the long-term, asset exchanges, global remittance networks, and foreign exchanges could all be moved to Blockchain through peer-to-peer lending. A widespread decentralized financial trading system has many unpredictable and far-reaching social, political, and ethical implications:

- Even though many roles will be made obsolete by the technology, jobs requiring the human element, such as performance improvement, IT risk, and other advisory roles, will grow in demand.
- Professional accountants are already preparing for an age where accounting and finance will be embedded in the Blockchain.
- Credible governance models will be required to be established to resolve oversight issues and ethical dilemmas. Blockchain's decentralization means that no one party can have control over the system. While this is useful for ensuring security and transparency, it raises questions regarding how large-scale changes to the program will be handled and who will make important ethical decisions.
- Proactively, Blockchain community is already responding to this issue. Associations like the Muskoka Group (created in August 2016), an assembly of Blockchain executives, and the Enterprise Ethereum Alliance are working collectively to address the platform's governance issues, and to prove that initiatives are underway to address these ambiguities.

Further, a 2016 study by IBM revealed that 65% of banks intend to rollout Blockchain solutions by 2019 (the company studied 200 global banks to arrive at this conclusion). Of those 200 banks, 15% said they wanted to integrate "full-scale, commercial Blockchain solutions" in 2017. From the study, it was also determined that 70% of early adopters are prioritizing Blockchain development to help create new business models and markets. It seems that banks and other intermediaries are turning the potential threats of Blockchain into opportunities to improve their own services. The financial technology industry is expected to grow beyond \$150 billion in the next 3-5 years.

According to a survey by the World Economic Forum, 10% of global GDP could be stored on Blockchain by 2025. Research and Markets (the largest market research database in the world) released a report in March, 2017, predicting that Blockchain technology will be used by up to 65% of enterprises by 2020. Likewise, a second IBM study that surveyed 200 financial market institutions, revealed that 14% of respondents said they would also like to implement scalable and commercialized solutions by 2017. Both the NASDAQ and the ASX have been working on launching their own Blockchains. These statistics and examples highlight that Blockchain is undoubtedly growing in momentum and that industries across-the-board are recognizing its potential. Blockchain platform is stirring up an unstoppable wind of technological change.

CASE STUDIES

Case Study 1

R3 - Interbank Reconciliation

Blockchains are designed to be useful in systems that require reconciliation between parties. Many of the major players in banking are backing the R3 consortium, which is researching the use of a Blockchain like distributed ledger for interbank reconciliations and other financial applications. Currently, millions per year are spent reconciling ledgers between banks; however, if a distributed ledger solution could be created that is able to handle the volume of transactions between the banks, then this could be greatly reduced.

This kind of application would be a private ledger, i.e., one where only invited parties can view the records or participate in creating new entries. However, it would require that interbank transactions are consolidated to form a single, authoritative record that all parties could verify. This could reduce the considerable efforts currently spent reconciling books with counterparties and, therefore, would allow for a more efficient banking system.

A solution of this kind is not feasible with the present implementations of Blockchain, either in volume or in speed, and indeed the R3 project has now morphed into other distributed ledger applications for the financial sector. However, if these significant challenges could be overcome, this is potentially a very impactful area of application for Blockchain. Others are looking at supply chain integration for similar reasons.

Case Study 2

Land Registry

Perhaps the clearest case for where Blockchain could be advantageous is provenance and transfer of ownership of assets, and land registry is a particularly good case. There have been several pilot studies and proofs-of-concept made, but none have reached full operational maturity yet. One proof-of-concept in this field was for land registry in Honduras, which has no current public land ownership registry and experiences difficulties with corruption and misappropriation; other projects have been proposed or developed in Georgia and Sweden, but none have yet reached large-scale testing. Creating a clear and permanent record of ownership and transfers of ownership would help create additional liquidity in the economy by increasing security, and fight corruption by distributing the maintenance of records to all parties rather than just to some.

As a public register, the open visibility of Blockchain is not an obstruction for land registry. It is acceptable for participants to see who owns, sells, and divides land; furthermore, the verifiability aspect can help to add transparency where needed. A land registry Blockchain would have to start by tokenising the land assets in question. i.e., creating a representation of each section of land as a legally-equivalent digital asset, stored on the Blockchain. This would be followed by making sure that the present owners had the ownership of the appropriate tokens assigned to them. This is no small undertaking as existing systems are already very complex, and there is a need to be flexible in future if existing land deeds are altered or split. What's more, if corruption in state officials are a concern, then getting approval from those same officials for a project that would reduce that corruption is challenging - and indeed this is what stalled the Honduras pilot scheme.

There is a larger lesson for Blockchain in this example – bitcoin works because it is a wholly online system, with all participants agreeing to the ownership and provenance records . But many other areas are more complex as ownership needs not only to be registered, but also tied to the real world. This causes problems in both directions, the register must reliably reflect real-world existence and condition of assets, and there must also be legal mechanisms for enforcing ownership rights when Blockchain records indicate these are held, even against parties who are not part of the Blockchain, or do not recognise it as legitimate.

If these challenges could be overcome, then a land registry Blockchain could thereafter record sales of land (or other similar transactions), creating a verifiable and permanent record. Furthermore, the distributed nature of the ledger would mean that neither downtime nor server failure would ever affect the availability of the service. While the costs of transacting on a Blockchain can be relatively high, for a low-volume, high value channel such as purchases and sales of land, they would likely be competitive.

Case Study 3

IBM Hyper Ledger

Hyperledger, a Linux Foundation project, is an open source community to help advance technology and thought leadership. It is deemed an “umbrella” for developer communities building open-source Blockchain and related technologies. Hyperledger was announced and formally named in December, 2015 by 17 companies in a collaborative effort created to advance Blockchain technology for cross-industry use in business. Now with over 130 members across the world, it is the fastest growing project in Linux Foundation history.

Hyperledger is curated by the Linux Foundation, which provides tools, training, and events to scale any open source project. IBM initially contributed what was then called Open Blockchain and is now called Fabric, and arguably that is the biggest/highest profile project. The idea is that Hyperledger rather than being a single platform (a la Ethereum) will be more akin to the Apache Project, with multiple projects under one umbrella that will be open source, freely available, and ideally have some measure of interoperability.

The vision of Hyperledger is to provide robust and efficient standards for Blockchain ledger technology to facilitate mainstream commercial adoption. Future applications will involve a world with many interconnected distributed databases and Blockchains, each of which will be specialized to suit the purpose of its users and will have the potential to communicate with other ledgers, as necessary.

Another goal for Hyperledger is to provide a modular Blockchain technology that contains a rich, easy-to-use application programming interface (API) and numerous core modules that enable easy development and interoperability. The API must be flexible enough to allow Blockchains built outside core Hyperledger to easily interact with their components and Blockchains. Further, Hyperledger believes that identity and patterns of behaviour of any party on a network must be difficult for unauthorized parties to ascertain by inspecting the ledger. Blockchain users must be able to make certain business logic and parameters of a transaction confidential, rendering them inaccessible to anyone other than the stakeholders.

Case Study 4

Dole Food Company, Inc.

The accounting and finance sectors are intricately connected; so much so, that delays in the financial reporting process and errors in record keeping and consolidation can have material impact on the buying and selling of company stocks. The stock crisis facing Dole Food Company Incorporated (Dole) can be studied to better understand this relationship and its relevance to blockchain. In 2013, Dole's CEO David Murdock decided to take the

company private. Stockholders argued that the shares were worth more than the \$13.50 that was paid out per stock. In 2015, the court ruled that the share prices were understated, and Murdock would have to pay an additional \$2.74 per share. This is where the issue emerges: When 4,662 shareholders filed their claims to receive the additional compensation, it was discovered that there were approximately 49 million facially valid stocks, yet Dole's accounting records only recognized about 37 million.

One of the explanations for the 12 million difference between the active shares and the record of stocks is the “chill” period instigated by the Depository Trust & Clearing Corporation (DTCC). Historically, the purpose of the DTCC has been to reduce the risks and costs of trade while improving market efficiency. The DTCC acts as a record keeper and clearinghouse for stocks. The problem, however, is that it takes three days to settle a trade, so during Dole's going-private merger, the DTCC “chilled” and did not record these trades. Despite that the closing date for the acquisition was on November 1, the DTCC's centralized ledger and subsequent accounting records did not receive information regarding transactions that took place on October 30, October 31, and November 1.

Therefore, if Person A sold a share to Person B on October 31, the DTCC still thinks Person A owns the share, while the brokers of Persons A and B know that Person B has now become the actual owner. Reconciliation becomes challenging because now a single share is facially valid to two different people (giving the illusion of two existing shares). Although the trades can be traced retroactively to identify the true owners, allocating the settlements becomes a lengthy and arduous process between the DTCC, 12 brokers, and share owners involved. This delay was once used to conduct audits to prove that investors actually owned what they claimed. However, as transaction speeds increased, this practice was eradicated, leaving an outdated system for trade.

The second issue responsible for the crisis has to do with the short selling of stocks. Short selling occurs when one party loans their shares to a second party. Then, the second party sells these shares to a third party, often at times without the first party owner's knowledge. When an event like this happens, it results in two beneficial owners because the first and third parties will claim that they are entitled to the settlement. This creates “phantom shares”: The illusion that there are more stocks issued than there actually are. In order to balance and reconcile this transaction, the short seller (the second party) would have to pay the first party the amount of the stock sold (or in other cases, the amount of the dividend). However, in the case of Dole, where over two years had passed, it became difficult to collect payment from the short seller for a variety of reasons. For example, the person may not have had an account with that broker anymore or the hedge funds may have been closed in the meantime. On October 31 alone, 2.9 million common shares had been shorted, with many more expected to have been sold on November 1 given that the common shares were trading for higher than the merger price. The Securities and Exchange Commission (SEC) inaugurated “Regulation AB” which stipulates that trustees must be given complete lists of stock beneficiaries, but because short selling creates two beneficial owners, this did little to mitigate the problem.

The misrepresented stocks in the case highlight that although the accounting and finance sectors rely on each other, the accounting that underlies the finance sector is often failing to keep pace. Ultimately, the two are not in sync with each other. The tale of the Dole stock crisis resurfaced in February 2017 when the judge overseeing the case issued a memorandum suggesting that this problem could have been averted by using blockchain technology. Blockchain could have prevented the situation in two ways:

- First, the current model is over complicated and expensive because it requires collaboration with the DTCC, custodian brokers, and the affected parties. The costs to settle, engage in a formal litigation process, or solicit help from the DTCC are costly for companies and raise red flags for investors. To put this into perspective, the DTCC charged a \$2,250 base fee to address the issue, with “additional consultation fees if difficulties arise”. In contrast, since all transactions are recorded in real-time on blockchain, the traceability, speed, and lower cost that the

technology provides makes it a more secure and efficient alternative to solving these types of problems.

- Second, the immutable aspect of blockchain would make it simple to identify the short sellers at any point in time. Cash could be collected automatically using digital currencies to avoid the risk of not being able to collect payment. Notwithstanding, even if a universal switch is not made to cryptocurrencies, blockchain still creates a transparent platform to track down the parties involved..Blockchain has the potential to realign these two industries by overcoming the obstacles created by the DTCC and short sellers. This translates to fast, traceable, and ethical transactions for investors.

CONCLUSION AND WAY FORWARD

Blockchain is an Internet of Values and Assets

As witnessed through Blockchain initiatives by first movers, this technology can be applied by professional service firms and other incumbents of the accounting industry to better meet client needs. In the years to come, Blockchain could be used regularly by professional accountants to manage a company's records, transactions, and performance. Triple-entry accounting, smart contracts, and automated taxation are just a few of the ways Blockchain can streamline accounting processes. While the technology has the potential to reshape capital markets as a whole, a dialectic still needs to be had regarding the social and political barriers impeding Blockchain's proliferation. Though no one can confidently predict the magnitude of Blockchain's growth, one thing is for certain, i.e., Accounting is just one block in the chain of industries being dramatically redefined by this disruptive technology.

There are still many unknowns with respect to how Blockchain will impact the audit and assurance profession, including the speed with which it will do so. Blockchain is already impacting auditors of those organizations using Blockchain to record transactions and the rate of adoption is expected to continue to increase. However, in the immediate future, Blockchain technology will not replace financial reporting and financial statement auditing. Audited financial statements are a cornerstone of business and play a key role in debt and equity financing, participation in capital markets, mergers and acquisitions, regulatory compliance, and the effective and efficient functioning of capital markets. Financial statements reflect management assertions, including estimates, many of which cannot be easily summarized or calculated in Blockchains.

Furthermore, the process of an independent audit of financial statements enhances the trust that is crucial for the effective functioning of the capital markets system. Any erosion of this trust may damage an entity's reputation, stock price and shareholder value, and can result in fines, penalties or loss of assets. Users of financial statements expect professional accountants to perform an independent audit of the financial statements using their professional skepticism. Auditors conclude whether they have obtained reasonable assurance that the financial statements of an entity, taken as a whole, are free from material misstatement, whether due to fraud or error. Blockchain as a technology will impact the processes adopted by assurance providers on financial statements, internal control framework and risk management system.

Professional accountants need to monitor developments in Blockchain technology because it will impact their clients' information technology systems. They should be conversant with the basics of Blockchain technology and work with experts to audit the complex technical risks associated with Blockchains. In addition, they should be aware of opportunities to leverage their clients' adoption of Blockchain technology to improve data gathering during the audit. They should also consider whether Blockchain technology will allow them to create automated audit routines. The auditing profession must embrace and "lean in" to the opportunities and challenges from wide spread Blockchain adoption.

REFERENCES

<https://www.3pillarglobal.com/insights/introduction-to-Blockchain-technology>

<https://www.Blockchain-council.org/Blockchain/what-is-merkel-tree-merkel-root-in-Blockchain/>

<https://bravenewcoin.com/assets/Reference-Papers/A-Gentle-Introduction/A-Gentle-Introduction-To-Blockchain-Technology-WEB.pdf>

<https://medium.com/fluree/Blockchain-meet-database-5eecaa38a358>

<https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/>

<https://inc42.com/features/watchlist-indian-Blockchain-startups/>

<https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/can-Blockchain-be-the-beachhead-for-indias-public-sector-profitability/articleshow/62957640.cms>

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2984126

http://iang.org/papers/triple_entry.html

<https://www.journalofaccountancy.com/news/2018/mar/how-Blockchain-might-affect-audit-assurance-201818554.html>

<https://www.ifac.org/global-knowledge-gateway/audit-assurance/discussion/Blockchain-will-impact-accounting>

<https://www.journalofaccountancy.com/news/2017/dec/Blockchain-for-management-and-auditors-201717994.html>

<https://njcpa.org/stay-informed/topics/article/2017/09/14/the-Blockchain-transformation-of-accounting-and-auditing>

<http://usblogs.pwc.com/emerging-technology/the-Blockchain-challenge/>

http://www.omgwiki.org/OMG-FDTF/lib/exe/fetch.php?media=designing_and_auditing_accounting_systems_based_on_Blockchain_and_dsl_principles.pdf

<https://www.icaew.com/en/technical/information-technology/technology/Blockchain/Blockchain-and-the-accounting-perspective><http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf>

<https://en.wikipedia.org/wiki/Blockchain#Predictions>

http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

COMPOSITION OF DIGITAL ACCOUNTING AND ASSURANCE BOARD 2018-19

Council Members

Chairman

CA. Atul Kumar Gupta

Vice-Chairman

CA. Manu Agrawal

CA. Naveen N. D. Gupta, President (Ex-officio)

CA. Prafulla Premasukh Chhajed, Vice-President (Ex-officio)

CA. M. P. Vijay Kumar

CA. Sanjay Vasudeva

CA. Debashis Mitra

CA. Dhinal Ashvinbhai Shah

CA. Anil S. Bhandari

CA. Prakash Sharma

CA. Mangesh Pandurang Kinare

CA. Dhiraj Kumar Khandelwal

CA. Babu Abraham Kallivayalil

CA. Jay Chhaira

CA. Nandkishore Chidambar Hegde

CA. K. Sripriya

CA. Mukesh Singh Kushwah

CA. Sanjiv Kumar Chaudhary

CA. Ranjeet Kumar Agarwal

Shri V. Kurian

Shri Sudhansu Pandey

Co-opted Members

CA. Arun Kumar Khowala

CA. Arun Kumar Agarwal

CA. Ashish Dua

CA. Kamal Sachdeva

CA. Pancham Ram Maurya

CA Sanjay Dashrath Patel

CA. Rajesh Loya

Special Invitees

CA. Parveen Kumar

Ms. Indumati Srinivasan

Prof. Neerav Nagar

Shri TVVPS Chakravarti T

Shri Jagannathan Chakravarthi

Secretary, DAAB

CA. Jyoti Singh





Digital Accounting and Assurance Board

The Institute of Chartered Accountants of India

(Set up by an Act of Parliament)

ICAI Bhawan, Hostel Block, 7th Floor
A-29, Sector-62, Noida - 2013 09 INDIA

Tel (Direct) +91.120.3045 961 / 992 / 963
www.cit.icai.org, www.pqc.icai.org