BLOCKCHAIN IN DATA ANALYTICS

EDITED BY MOHIUDDIN AHMED

Blockchain in Data Analytics

Blockchain in Data Analytics

Edited by

Mohiuddin Ahmed

Cambridge
Scholars
Publishing

Blockchain in Data Analytics

Edited by Mohiuddin Ahmed

This book first published 2020

Cambridge Scholars Publishing

Lady Stephenson Library, Newcastle upon Tyne, NE6 2PA, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN (10): 1-5275-4429-X
ISBN (13): 978-1-5275-4429-1

Dedicated To

"My Loving Parents & Wife"

—Mohiuddin Ahmed

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I am grateful to the Almighty Allah for blessing me with the opportunity to work on this book. It is my second time as book editor and my sincere gratitude to the publisher for facilitating the process. This book editing journey enhanced my patience, communication and tenacity. I am thankful to all the contributors, critics and publishing team. Last but not least, my very best wishes for my family members whose support and encouragement contributed significantly to complete this book.

—Mohiuddin Ahmed
Academic Centre of Cyber Security Excellence,
School of Science,
Edith Cowan University, Australia

PREFACE

Introduction

Blockchain is a public ledger where transactions are nearly impossible to amend. A decentralized database where business is transparent without any involvement of the middleman. The first use of blockchain technology was the digital currency (bitcoin). However, other potential uses of this technology are yet to be explored. It is expected to have an impact on cyber security, internet of things, supply chain management, market prediction, governance, information management, financial transactions and more application domains. Till today, blockchain has redesigned the way people deal with their money due to its effectiveness, especially in terms of security. Therefore, from the data analytics point of view, investigation of blockchain technology in a wide range of applications domain is crucial. In this context, this book will provide a broader picture on the concepts, techniques, applications, and open research directions in this area. In addition, the publication is expected to serve as a single source of reference for acquiring the knowledge on this emerging technology.

Objective of the Book

This book is about compiling the latest trends and issues about emerging technologies, concepts and applications which are based on Blockchain. It is written for graduate students in universities, researchers, academics, and industry practitioners working in the area of Cyber Security, Data Science and Machine Learning.

Target Audience and Content

The target audience of this book is composed of graduate students, professionals, and researchers working in the field of data analytics and cyber security in multi-disciplinary applications. The chapters are written in tutorial style so that the general readers can be able to easily grasp some of the ideas in the relevant areas.

SECTION I: Blockchain Introduction
Chapter One: Introduction to Blockchain

SECTION II: Blockchain Concepts
Chapter Two: BlockChain for Internet of Things
Chapter Three: Blockchain and Industry 4.0
Chapter Four: Blockchain and Fog Computing: Fog-Blockchain Concept, Opportunities and Challenges
Chapter Five: A New Era of Project Management using Blockchain Technology

SECTION III: Blockchain Applications
Chapter Six: Blockchain Technology for Protecting Personal Information Privacy
Chapter Seven: Blockchain-enabled entrepreneurial financial funding and investments: The new era of Initial Coin Offerings
Chapter Eight: AI-enabled IoT Network in Agricultural Food Chain using Blockchain Technology
Chapter Nine: Exploring e-commerce in cyber security context through Blockchain Technology
Chapter Ten: Blockchain in Health Care

The first section includes an introductory chapter to discuss blockchain. The second section has four chapters which reflect on the different concepts of blocckchain for data analytics such as Internet of things, Industry 4.0, fog computing and project management. These topics are considered as emerging trends for blockchain data analytics. The third section is dedicated for the applications of blockchain for data analytics in different domains such as privacy, healthcare, finance, e-commerce, agriculture etc.

Editor
Mohiuddin Ahmed

CHAPTER ONE

INTRODUCTION TO BLOCKCHAIN

MD. SAEF ULLAH MIAH[1],
MASHIOUR RAHMAN[2],
MD. SADDAM HOSSAIN MUKTA[3]
AND ANEEM AL AHSAN[2]

[1]University Malaysia Pahang, Malaysia
[2]Department of Computer Science, American International University-Bangladesh
[3]Department of Computer Science and Engineering, United International University, Bangladesh

Abstract

Blockchain is one of the most-hyped topics of the computing world recently, as well as in the financial technology (FinTech) industry. Experts say that the future of monetary transactions, and secure information exchange rests on the shoulders of blockchain. Blockchain provides the potential to change how the world moves forward. For example, if you want to buy any asset, such as a house, vehicle, or any other tangible or intangible property, you currently need to go through a lot of paperwork and labor-intensive effort. However, blockchain makes life easier, and accomplishes these cumbersome functions within a short period of time. Blockchain can be defined as a simple block of transparent digital information which is highly secured and shareable, but immutable. Transparent digital information means the data exploited is traceable and identifiable. In this chapter, we present briefly what blockchain is, how it works, and what the major application areas in the real world are.

Keywords: Big Data, Blockchain, Cryptography, Data Analytics, Digital Currency, Information Security, Internet of Things, Private Key, Public Key, Transaction.

1. Introduction

Blockchain is one of the most recent technologies in the domain of security, tractability, and transparency, for managing any digital asset transaction, as well as for physical assets and agreements.

In this chapter, we will learn about blockchain, how it works, and what the benefits and limitations of blockchain are, as well as the area of blockchain implementation, from which we can gain the advantages of blockchain. Section 1 describes the basic idea of blockchain, and later, in section 2, the history and evolution of blockchain are depicted. Section 3 covers the types of blockchain, followed by Section 4, which describes the basic mechanisms of blockchain and transaction. Section 5 focuses on the importance of blockchain, Section 6 presents the applications of blockchain, and finally, Section 7 provides the challenges and opportunities of blockchain.

We have the conception that blockchain is the technology that powers bitcoin, and although this was its original purpose, blockchain is capable of so much more. Let's see what blockchain is.

Blockchain is shorthand for a suite of distributed ledger technologies that can be programmed to record and track anything of value, such as financial transactions, medical records, land titles, and so on. Blockchain technology is based on the centuries-old method of the general financial ledger. In simplified language, it is a digital ledger which holds the records of all sorts of transactions that happen in a peer-to-peer network. This technology is assumed to 'cut out the middleman' from any sort of transaction or transfer of digital assets. This is a much more secure and decentralized medium. Financial institutions are exploring the possibilities of using this technology to ensure secure transactions.

Blockchain works like a digital ledger, with some particular characteristics, such as:

- Blocks can only be appended;
- No block can be edited;

- The validity of any transaction depends on the previous transaction, so that no fraud can happen;
- Transaction happens only after full verification.

The working mechanism of blockchain will be described later in this chapter.

2. History and Evolution of Blockchain

The history of blockchain is not that old. The first step of blockchain was initiated in 1991 by Stuart Haber and W. Scott Stornetta, with their work on a cryptographically-secured chain of blocks, where no one could tamper with the time stamps of documents. In 1992, they upgraded their system to incorporate Merkle trees, to allow the system to accept more documents in a single block. [1] However, the blockchain that we know today was introduced by Satoshi Nakamoto in 2008. He is known as the brain behind blockchain technology. Many people believe that he could be the person, or one of a group of people, who worked on bitcoin for the first publicly-known application of digital ledger technology (DLT). [2][3] Satoshi released a white paper on blockchain, explaining all the details of the technology in 2009, and from there, the development of blockchain has gone far, with many implementations.

Evolution:

The evolution of blockchain can be divided into three different phases: Phase 1, Transactions; Phase 2, Contracts; and Phase 3, Application. [1] Figure 1 briefly presents the timeline of the evolution of blockchain.

Phase 1: Transactions (Blockchain 1.0 and Bitcoin):

The timeline of this phase is from 2008 to 2013. During this time, Blockchain 1.0 was in practice, where the main goal was to carry out peer-to-peer transactions. During this phase, bitcoin was the popular implementation of blockchain technology, and everyone was busy with bitcoin transactions and bitcoin mining.

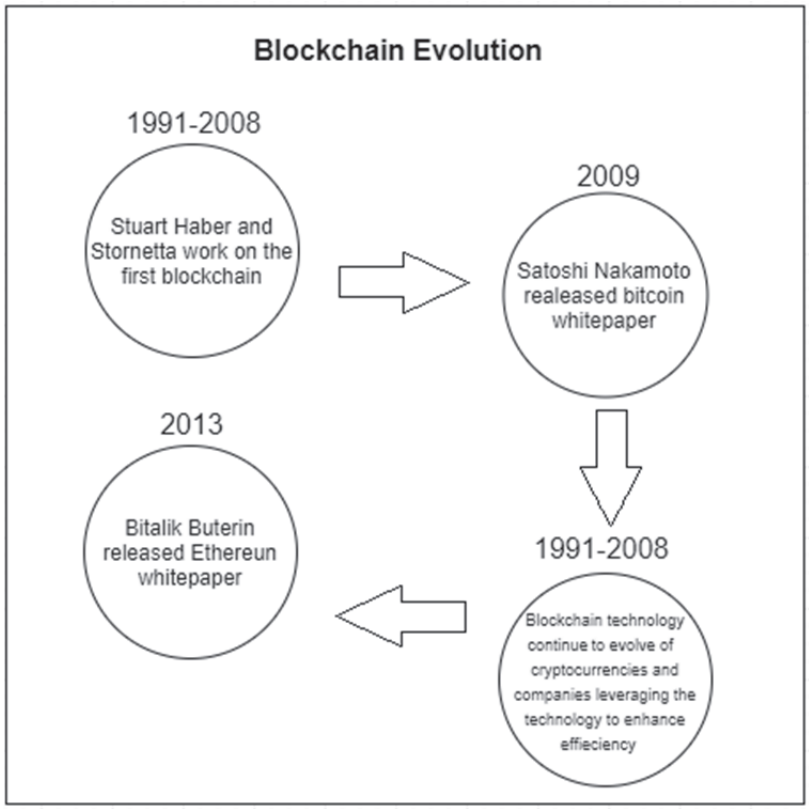


Figure 1: Evolution of Blockchain

Phase 2: Contracts (Blockchain 2.0 and Ethereum):

The timeline for the phase of contracts actually appears between the years of 2013 and 2015. In this phase, another potential of blockchain technology was noticed. Decentralization was the key feature of this phase. While in the transaction phase, the communication was mostly on a peer-to-peer basis, but here, it was used in a distributed fashion, and the technology of smart contracts was widely used. Smart contracts expanded blockchain from being used as a cryptocurrency to a platform of decentralized applications.

Vitalik Buterin was one of the developers who figured this out. He started building a new public blockchain network, named Ethereum, which can perform various functions in addition to being a peer-to-peer network. This version of blockchain technology can be named Blockchain 2.0. The Ethereum blockchain evolved to become one of the biggest applications of blockchain technology during this phase.

Phase 3: Applications (Blockchain 3.0 and the Future)

The history of blockchain does not stop with bitcoin and Ethereum. In recent years, a number of projects have come up with new features for blockchain. Phase 3 started from 2018, where different applications began to be integrated with blockchain technology, and blockchain was being secured with biometric complementation, such as facial recognition, voice matching, and fingerprints. The network of connected devices known as the internet of things (IoT) is being aggregated to blockchain platforms, and more new platforms and applications have started using blockchain in their daily operations.

3. Types of Blockchain

There are three types of blockchain, known as public blockchain, private blockchain, and consortium blockchain [6].

- **Public Blockchain**

  The public blockchain network is open access. The network imposes no restriction to access its premises. Anyone can send a transaction to this network, and anyone can become a transaction validator. [6] Usually, the public blockchain network offers economic incentives for the people who secure them, and utilizes some sort of proof of stake, or proof of work, algorithm, to general people. This is known as cryptocurrency mining. Some of the largest and best known public blockchains are bitcoin and Ethereum.

- **Private Blockchain**

  Unlike the public blockchain network, private blockchain networks are permissioned, which means no one can join the network until they are invited by the network administrator [4]. Both participants' and validators' access are restricted without any invitation to participate. This sort of blockchain network is used by companies who want to

secure their data without sacrificing autonomy or taking the risk of exposing data to the public internet.

- **Consortium Blockchain**

Similar to the private blockchain network consortium, the blockchain network is also permissioned and semi-decentralized, but instead of a single organization controlling the network, a number of companies might each operate a node on such a network [5][6].

4. How Blockchain Works

In order to understand how a blockchain chain works, let us discuss a common scenario where it can be operational, and some of its key attributes. The main purpose of blockchain is to provide security, and banking transactions are the most suitable candidates to use blockchain. Let us consider that a financial transaction in the form of a money transfer is taking place between an account named 'A' and another named 'B'. It is essential that both the accounts are updated after the transaction is completed. This is the place where intruders may interfere and cause changes to the entries that are made on both the accounts while updates are performed, leading to the possibilities of a tampered-with transaction. In order to address this situation with a feasible solution, blockchain is used. Some of the following paragraphs will describe in detail about how the solution can be achieved, relying on the fact that it is a collection of blocks linked with each other in chronological order, and each block contains a set of data. However, let us take a closer look at how blockchain is better than traditional processes, in order to understand its operation. This can be explained based on some key attributes which are as follows:

- Peer-to-peer – There is no central authority who has control of the entire data. All participants within the network are allowed to communicate with each other directly;
- Distributed – All the blocks are distributed over the entire network, which makes it difficult for intruders to tamper with the data;
- Add-Only - Data can only be added in the blockchain in time-sequential order. This property implies that once data is added to the blockchain, it is almost impossible to change that data, and it can be considered practically immutable;
- Consensus – This is the most important attribute of all. It gives blockchain the ability to update its data via consensus. In this way,

no central authority has control over the data. Any kind of update has to be made following strict protocols, and will be only added when a consensus has been reached among the peers in a network.

Blockchain is made up of several sets of data blocks which hold the records of each transaction. Every block is connected with every other. Blockchain can be either private or public. In a private blockchain, only members are allowed to access the network. Anyone can use a public blockchain network, like the internet. Blockchain uses cryptographic technology to secure the transactions, and cryptography is a mathematical method which keeps data secure by proving its identity mathematically. Blockchain uses two keys for this purpose. The first one ensures only a valid user can enter a transaction block to the existing blockchain, and another key will let someone else authenticate whether a valid user has made this block or not.

Another important mechanism that is used in blockchain is immutability. That is, no tampering or editing of previously made blocks is possible in blockchain. It is controlled by a cryptographic concept known as hash. Hashing makes data secure by altering data into something else, using mathematical functions. For example, the hash of the sentence "the quick brown fox" is "9ECB36561341D18EB65484E833EFEA61EDC74B84CF 5E6AE1B81C63533E25FC8F" using SHA-256 encoding. If only one letter of the alphabet is changed in the previous sentence, then the hash will turn into something completely different from this one. In the blockchain, any minute change is detected, as hashes are linked to each other. A new block must have the previous block's hash linked to it. As a result, though it is public, it is very secure. Working Mechanism of a Blockchain Transaction is listed below:

1. When a transaction is carried out, it is linked to the blockchain as a block, protected by cryptographical encoding. All the blocks created within a certain time are sent to the other members of the network. In bitcoin, all transactions are sent within 10 minutes.
2. Members of the network with high computing-power-enabled devices, or computers, compete with each other to validate the transaction, by solving a complex problem. Any member who solves the problem first, receives a transaction fee, or another reward. For example, in bitcoin's blockchain, members receive bitcoins.

3. Any block which is validated is first time stamped, and is then added in order. Newly validated blocks are added to the previously validated blocks.
4. The entire chain of such blocks is called blockchain, which keeps updating with newly added blocks. Figure 2 describes step-by-step how blockchain makes a transaction.

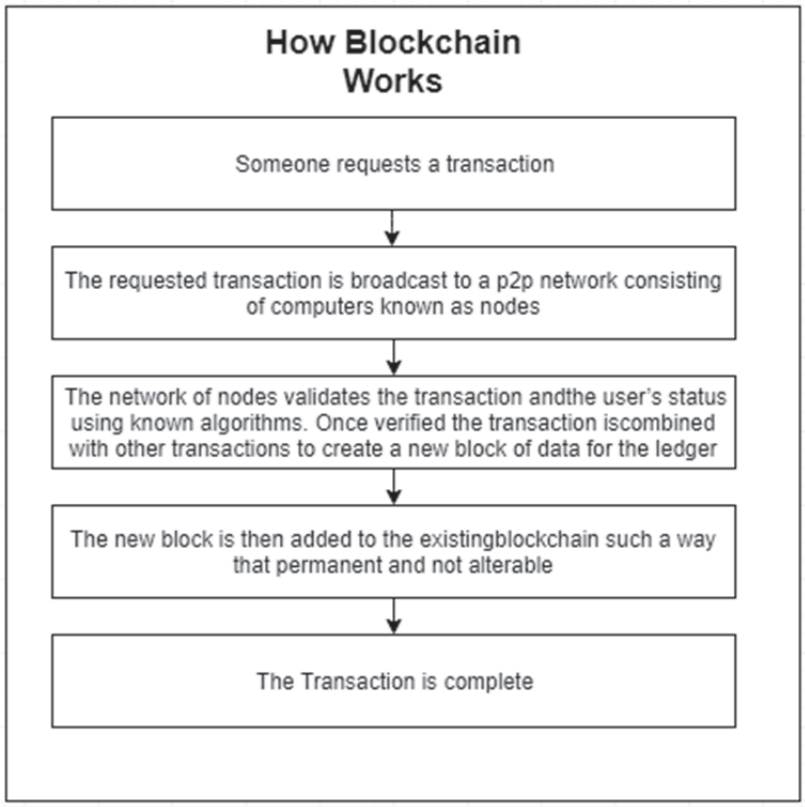


Figure 2: How a blockchain transaction works

5. The Importance of Blockchain

The importance of blockchain relies on its primary features, which are trust, integrity of content, smart contract, and bypassing the intermediary, in any sort of transaction. Blockchain technology is changing industry

drastically, especially industries which are related to financial technologies (FinTech). Besides FinTech industries, blockchain has brought changes to healthcare industries, e-governance systems, and data analytic-based industries. The importance of blockchain is not easy to describe in words, except by experiencing it first-hand.

Let's look at some real-world problems and scenarios which can be solved by using blockchain technology. The Australian Securities Exchange recently scrapped their old CHESS transaction system for managing the stock exchange market, for distributed ledger technology (DLT). [8] The Government of Andhra Pradesh in India plans to deploy blockchain technology across the administration. They have piloted two projects - managing land records, and streamlining vehicle registrations, using blockchain. [7] These are just examples; many others are switching to blockchain technology for solving different sorts of problems, and many are on their way to embracing it. The healthcare industry is another example where blockchain is being used for efficient and secured data management problems which are shared across different healthcare providers.

The electoral process is also a beneficiary of blockchain technology, which can provide an extra layer of security that the current manual system cannot provide. Blockchain is also being tested in the management of supply chains, insurances, peer-to-peer lending, energy sharing systems, gaming and streaming systems, and so on. Blockchains are also being used to solve daily life problems; for example HelloTickets is a platform which publishes tickets for events. Using blockchain guarantees each ticket's authenticity, removing the necessity of a third party to authenticate the tickets. The possibilities of blockchain are so huge that many governments are taking interest in it. For example, Spain's Securities Regulator has undertaken a pilot project, the President of Uzbekistan has signed a decree on blockchain integration, and the Maltese parliament has passed laws which set a regulatory framework for blockchain, cryptocurrencies, and DLT [9].

What if there was no blockchain? What would be the consequences of that? We might possibly face a lack of trust in any sort of online transaction, more fraudulent activities in asset management, especially in land titles, and a fear of not getting original and authentic data. We might also face a lack of efficiency in large transactions and service delivery systems.

Cheng et al. proposed a business model for the decentralized electricity market, based on blockchain, in order to reduce the high cost of achieving a digital centralized solution for construction, management, and maintenance [17]. Since the management of data which is produced in large quantity is difficult and costly, blockchain was used as a solution, in order to achieve peer-to-peer transactions in the power system.

Metler demonstrated the use of blockchain in the healthcare industry, [18] stating that it can add significant value to the treatment of older people, or of chronic diseases. A startup in the USA, called Gem, has used Ethereum blockchain to create a health network [19]. This will allow healthcare specialists to be present in a large distributed network system, where it is possible to share multiple copies of different kinds of information with each other. It will help to combine business, individuals, and experts, at the same time, which has the potential to increase patient care. This also means that the records of individual patients, and their interactions with doctors, will be present in the network for others to see when needed. This means that patients will be exposed to a reliable healthcare environment. In another attempt, Estonia collaborated with Guardtime to digitalize its healthcare system, where all the medical records of citizens were available [20]. The entire system was developed using blockchain, which helped to retrieve medical information when required by any individuals, especially in the case of insurance.

When more and more people are implementing systems within systems, more and more data is emerging which can be used for various types of research. Healthbook is a Swiss digital system that efficiently stores and manages health data [21]. This has led to the availability of numerous health data, based on which, different medical research were performed. Blockchain also has wide application in the pharmaceuticals industry. For the production of any kind of drugs, the final product must maintain the required quality in order to be used commercially. For this process, data can be used to monitor the production of drugs to ensure quality.

According to the World Health Organization (WHO) the amount of counterfeit drugs has risen by up to 30% in developed countries. Some of these drugs are also used for cancer, antibiotics, painkillers, contraception, and other diseases. As a result people are badly affected. Hyperledger, which is a research network across industries, launched the Counterfeit Medicine Project, [24] which uses blockchain to detect such counterfeit

drugs. Apart from healthcare, there are other sectors where there are influences of blockchain.

Tam Vo et al. proposed a system that will transparently manage and analyze data for car drivers in developing countries, in order to introduce a 'pay-as-you-go' insurance service [22]. The reason for proposing this system was that drivers have to pay a large amount of insurance, independent of mileage, and driving behavior and patterns.

Nguyen provided a study using blockchain for economic growth [25]. He derived that blockchain can contribute to journalism, since the contents can be made available online, and interested persons can buy the contents by paying a few cents. This, in turn, encourages publishers and writers to create more content maintaining proper writing quality, as people have so many options to choose from. So a new source of earning is being created, and writers are discouraged from providing fake information, as the contents are available to everyone. In addition to writers, with its wide spread of data all over the network, blockchain can provide anyone with a platform to earn, from artists to game producers. Nguyen also adds that the use of blockchain also promotes new forms of media, such as crowd-made RPGs (real-life prediction games), online interactive drama, and novels, as well as new ways of combining art, music, and storytelling. He also concluded that the monopoly of the cable TV companies can be broken, as content is available online, and users usually have to pay only a little to view it.

Hou discussed the importance of blockchain for e-governance in China [26]. He concluded that, along with the help of blockchain, e-governance will help with the quality and quantity of government services, government information will be transparent and available to the citizen, different government organizations can easily share information between themselves, and China will get help to build its own credit system.

Who does *not* need blockchain? The answer to this common question is that if any application does not need to store the state, there is no involvement of multiple parties, and no need of public verifiability, then the application is not meant to use blockchain technology. The flowchart provided below will come in handy to understand the scenarios where blockchain is not needed. [10]

6. Applications of Blockchain

There are numerous fields where we can use blockchain, but for now we will be limited to the following fields, and all of them will be elaborated in different chapters of this book.

6.1 Data Analytics

Data analytics (DA) is the process of examining sets of data to draw conclusions about the information they contain. This means finding actionable information from large data sets. Recently, data is being transformed into currency, and data analytics is at the root of this shift. [11] Data analytics are used for future prediction, and are being used by companies from financial management to marketing. But using data in such a way to extract trends and information comes with high barriers, such as trained specialists and pricey equipment. With the use of blockchain, these can be lowered to the least cost. Blockchain is the way to minimize the data analysis cost for large data sets, with distributed networks of different machines and algorithms.

6.2 Big Data

Big data refers to data sets that are too large or complex for traditional data processing application software to deal with efficiently. So far, we are familiar with data analytics, and data analytics also deals with big data. While using blockchain for data analytics, it adds another data layer to the big data analytics process. This data layer provides two additional values to big data, [12] and those are:

1. Blockchain-generated big data is secure, as it cannot be forged due to the network architecture;
2. Blockchain-based big data is structured and complete, which makes it perfect for further analysis.

Big data, combined with blockchain, can lead to lot more efficient analytics. There are three reasons for this. [33] These are as follows:

- Security – Every single record inside a block in a blockchain is highly secured, which makes it very difficult for any data to be tampered with;
- Transparency – The data can be traced back to its point of origin;

- Flexibility – Blockchain can store both structured and unstructured data.

The main facts about combining big data with blockchain are the quick transfer of data, and the overall improvement of the stored data. Blockchains will allow businesses to confidently identify the integrity of the data being generated. Consensus-driven timestamping, proper audit trails, and immutable entries, will all become better, as blockchain starts becoming more mainstream. Healthcare is one of the sectors which is supposed to receive a considerable number of benefits. Healthcare providers can share information with patients, their physicians, insurance providers, justice departments, employers, etc., easily and securely. This can lead to:

- Following up the patients properly;
- Ever-available medical records that cannot be altered;
- Ever-available, secure, patient history.

6.3 Information Security

The future of information security, or cyber security, relies on blockchain technology. As blockchain technology allows the blocks to be decentralized with data integrity, it can be used to prevent any type of data breach, identity theft, cyber-attack, or any other fraudulent activity in any transaction. What can be done by using blockchain in information security is listed below: [13]

1. Protected edge computing with authentication;
2. Advanced confidentiality and data integrity;
3. Secured private messaging;
4. Improvement of public key infrastructure;
5. Intact domain name system;
6. Diminished DDoS attacks.

More information can be found in the relevant chapters of this book.

6.4 The Internet of Things (IoT)

Traditional IoT systems are based on centralized architecture, where information is sent to the cloud from devices, and after processing, sent back to devices again. With billions of devices, this architecture is not

scalable while maintaining the security of data, and with the provision of third parties to authenticate data on each transaction, the system will be incredibly slow.

Blockchain is, by default, a cryptographically secured distributed ledger system which allows a secure data transaction system between different parties. Smart contracts in the blockchain network will allow devices to function securely and autonomously. It not only allows greater automation, scalability, and cheaper transfer (as there is no third party), but can also prevent data tampering by individuals who want to use the data for their own benefit. The architecture is also decentralized and cryptographically secure [14]. Moreover, with a centralized network, the risk of a single point of failure is also mitigated in the blockchain-enabled network. IOTA is an example of a blockchain-based IoT platform.

6.5 Cyber Physical System/Smart Grid

A cyber physical system (CPS) is a mechanism that is controlled or monitored by a computer-based algorithm, and tightly integrated with the internet and its users. As an example, we can mention any autonomous industrial production system. In such a system, the hardware, users, and software, are tightly bonded, and the following challenges are faced over time: [15]

1. Heterogeneity in devices and resources;
2. Multiple attack surface;
3. Scalability;
4. Centralization;
5. Lack of control over data sharing and lack of auditability;
6. Complex interaction of different OS, software stacks, and hardware;
7. Different implementation of security or privacy mechanism.

By integrating the great features of blockchain technology, we can provide solutions to the above-mentioned problems of any cyber physical system. The features we would like to use to solve these problems are, the distributed nature of blockchain, chronological and time stamped records, immutability, auditability, and cryptographically sealed data transfer.

6.6 E-governance

There is particular interest in many countries in using blockchain for e-governance, in order to reduce infrastructural and communication costs, and also to build a reliable and transparent governing system [27]. For a country where the government is trying to digitize its services, blockchain can be the most suitable option. If implemented properly, e-government can allow the citizens, organizations, and enterprises, to carry out their task properly and with a lower cost. When the government is trying to introduce new services for food or healthcare or any other sectors, the use of a blockchain is always imminent for its distributed architecture, encryption, data immutability and transparency.

Some countries face continuous threats from counterfeit drugs. The most significant reason is the lack of regulation. The drug might not be properly packaged, or it is illegally sold in independent corner markets. In such cases it is also difficult to find out whether a drug is real or counterfeit. One current solution that is being tested is government working with the pharmaceutical companies to code drug packages in such a way so that consumers can later use this code to verify whether the drug is legitimate by using text [27]. Blockchain was used to build the network for this communication.

Kenya and Ghana are trying to apply blockchain to keep trace of their land records. Another land record keeping system has been implemented successfully in Georgia. Estonia has applied blockchain technology for business registration, e-health records, and other applications. Dubai has three pillars of government efficiency, industry creation, and international blockchain leadership, as part of its Smart Dubai initiative, and recently incorporated blockchain as part of its online payment portal, DubaiPay.

6.7 Education

It is a common belief that blockchain is only associated with providing security to any particular network. However, now we have explored other fields which can also utilize the benefits of this technology. Education is an equally important sector, comparable to the others discussed, which also uses blockchain. Editech is quickly growing, with the expectation of reaching a net worth of $93.76 billion by 2020. [28] Blockchain technology can formulate an entire transcript for a student. [30]

Duan et al. proposed a blockchain technology based on learning outcomes. [29] This technology is dependent on the graduation requirement index of the university with professional certification, and uses automated evaluation software as a tool. The records of each block are: the learning outcome, value, qualitative and quantitative combination of grades, process and evidence, the course name, the learning outcome name, and the weight of the course. Later, these records are used to convert the result of the students, according to the traditional grading system, into a capability index evaluation result. The University of Nicosia uses blockchain to manage all student certificates received from MOOC platforms [31].

Sony Global Education created a global platform to store information related to different degrees in one place [32]. One other most important application of blockchain is to store the information of students who have passed, carefully. Since it provides a large repository data along with efficient security, data can be saved and retrieved whenever required.

6.8 Crowd funding

Projects like Weifund are looking for ways to implement a crowd funding system using blockchain [34]. The main idea is that the decentralized nature of blockchain allows for the creation of multiple smart contract templates for launching individual contracts. Users can also create their own campaigns. By using smart contracts, two communicating parties can securely and easily transfer information and money amongst each other, without the involvement of any third parties.

6.9 Sports

In Sam Mire, "Blockchain for the Sports Industry: 11 Possible Use Cases"(2019), [36] some statistics are given. These suggest that, in 2018, attendance at major baseball games dropped by 8.6% of the rate achieved in 2017. The national football league also faced a 2% decline in annual attendance and a 10% decline in ratings. However, there was sharp increase in e-sport, where humans compete through digital, video, or game representation. An annual increase of 124 million viewers is expected between 2016 and 2020. This is a clear indication of generational differences, and decision makers for the traditional sports market must find ways to make clubs, athletes, leagues, and individual match outcomes, more attractive, keeping the venue experience affordable. Blockchain can

be one possible solution, through live sports betting and fantasy sports platforms. Other uses of blockchain include transparent reputation management for teams, leagues, and individual athletes, and a general reduction in middlemen, through automation, to make match attendance more affordable. Some applications are as follows:

- Tokenizing athletes – Through this technique, blockchain is used to invest in low-earning baseball players who agree to share an amount of their future earnings with the investors. This technique was introduced through the Big League advance, by Michael Schwime [36].

- Smart tickets to end scalping – The increase of e-ticketing systems has shown an increase in the number of online ticket vendors. This led to the selling of fake tickets. As a solution to this, blockchain was introduced, to bring all the authentic ticket-selling vendors together in one place, so that users can easily buy tickets from trusted sources.
- Decentralizing ticket resale/sharing – There are policies to return 100% of the money used to buy tickets, if someone does not receive them in time. However this will not alter the experience of watching a live game. Reasons for the tickets failing to reach the buyer on time can be transportation delays, or the purchase of tickets just a few days before the game. As a solution to this, blockchain can be used to deliver copies of smart tickets whenever they are bought.

- Recording and sharing performance data properly – Since blockchain is a reserve of data, it can be used to record data from different matches, which can later be used to provide various insights. These insights can be how a player performed in a match, and, based on other factors, what improvements can be made to performance. Also what the possible playing strategy might be to help a team win a match.

- Decentralizing the payment procedure of Fantasy Sport participants – Since this requires an online transaction, providing security is a difficult task. As Sam Mire notes, “The industry is pegged at roughly $7.22 billion in total, including money spent on ancillary activities, such as draft parties, food deliveries, fantasy-related memorabilia, etc. Offices, schoolyards, and group chats have all

become the domain of fantasy sports players, who enjoy the competition amongst friends, and the ability to make virtually every game more interesting" [36]. As a result, providing security for transactions is important, and blockchain can be used as a solution.

7. Opportunities and Challenges

Blockchain technology has a lot of opportunities and potential in every service which involves data and transactions of data. This is not limited to FinTech industries, banks, E-commerce, mobile commerce, cloud data services, end-to-end messaging services, data analytics, the internet of things, healthcare industries, medical data sharing infrastructures, and cyber physical systems. Besides these mentioned fields, we have witnessed other, different, implementations of blockchain technology. Blockchain also creates several new employment positions in industry, as follows:

- Blockchain Developer – The responsibilities are mainly comprised of designing, implementing and supporting a network that will be developed using blockchain through the various stages of production and development. There will also be other tasks that will include analysis of requirements, blockchain technology design around a certain business model, researching new technical solutions and protocols, creating and automating blockchain development workflows, implementing test-driven development practices, and building and launching a blockchain network.

- Blockchain Engineer – The blockchain engineer works on creating blockchain infrastructure, building end products on top of it, and developing meta transaction infrastructure using mobile applications, as well as development around document-signing frameworks and associated infrastructure, and development of APIs that interface with the blockchain.

- Blockchain Platform Engineer – The blockchain platform engineer provides expertise and development support to blockchain initiatives throughout the company, and develops subject matter expertise on blockchain network platforms, architectures, and administrative/operational requirements. He/she designs and builds

back-end blockchain functionality, i.e. network infrastructure, consensus algorithms, smart contracts, and identity authorities.

- Blockchain Protocol Architect/Director – The architect/director works with governments to build a blockchain identity and credit-scoring system to enhance financial security. He/she builds a global multi-tenant platform, that includes scaling across the world, and partners with other distributed systems engineers to develop a highly scalable cloud-based system. He/she brings thought leadership around blockchain across the organization, and externally, to continue to develop the engineering brand.

- Software Engineer – The software engineer builds networks such as a food quality tracking blockchain, used to record and validate assertions about quality food production, packaging, transport, and final use. He/she builds a new generation of high-performance blockchain focused on optimized smart contract execution, and develops a crowd-funding blockchain.

Besides these opportunities, blockchain also addresses some challenges which are mentioned below: [16]

1. Blockchain is a complex technology which includes lots of cryptographic algorithms and operations which are not always easy for general people to understand;
2. Blockchain requires a large network of users to work efficiently;
3. Blockchain includes transaction costs and requires a good network speed;
4. Blockchain has one notable security flaw, which is known as 51% attack. 51% attack is when more than half of the computers working as nodes to service tell a lie, and so it becomes truth. But the solution to this problem has already been addressed.

Several new algorithms and measurements have been taken to combat the challenges, opening up new horizons in the research into information security.

References

[1] Goyal, S. “Blockchain Technology History: Ultimate Guide”. Online access: February 1, 2019, See at: https://bit.ly/2Zt1tSK

[2] Marr, B. A Very Brief History Of Blockchain Technology Everyone Should Read. Online access: February 1, 2019, see at: https://bit.ly/2IjIl3R
[3] Popovski, L., & Soussou, G. (2018, May 14). A Brief History of Blockchain. Online access: February 1, 2019, see at: https://bit.ly/2FbJrg2
[4] Bob Marvin (30 August 2017). "Blockchain: The Invisible Technology That's Changing the World". PC MAG Australia. ZiffDavis, LLC, September 2017.
[5] Blockchain. (2019, February 05). Retrieved January 25, 2019, from https://en.wikipedia.org/wiki/Blockchain
[6] Khatwani, S. (2018, September 15). Different Types Of Blockchains In The Market and Why We Need Them. Online access: January 20, 2019, see at: https://bit.ly/2HETqdL
[7] TNM Staff (2018, February 17). AP govt becomes first state in India to adopt blockchain tech for governance. See at: https://bit.ly/2KROCVX
[8] Crofts, B., Lam, D., & Kosmatos, J. (2018, September 24). Solving real world problems with blockchain. Online access January 20, 2019. See at: https://pwc.to/2IO7SBj
[9] Black, S. (2018, July 05). Here's a great example of a company using Blockchain to solve a real problem. Online access: January 20, 2019. See at: https://bit.ly/2Fbv5wf
[10] ElSeidy, M. (2018, August 29). To Blockchain or Not To Blockchain – Hacker Noon. Online access: January 30, 2019, See at: https://bit.ly/2IKbwvX
[11] Brooke, S. (2018, June 26). How Will Blockchain Make Predictive Analytics Accessible? Online access: February 2, 2019, See at: https://bit.ly/2MOzMCd
[12] Fedak, V. (2018, February 21). Blockchain and Big Data: The match made in heavens – Towards Data Science. See at: https://bit.ly/2FbsMJE
[13] Sharma, T. K. (2018, September 25). The Future of Cyber Security: Blockchain Technology. Online access: February 4, 2019. See at: https://bit.ly/2IlLXm1
[14] Pauw, C. (2019, February 12). How Significant Is Blockchain in Internet of Things? Online access: February 4, 2019. See at: https://bit.ly/2WIGbhS
[15] Blockchains for CyberPhysical Systems: Applications, Opportunities and Challenges [Web log review]. (2018, September 06). Online access: February 06, 2019, See at: https://bit.ly/2MPRW6O

[16] Bauerle, N. (n.d.). What are Blockchain's Issues and Limitations? Online access: December 25, 2018. See at: https://bit.ly/2RjobJ9
[17] S Cheng, B Zeng and Y Z Huang (2017) 'Corrigendum: Research on application model of blockchain technology in distributed electricity market', *Conference Series: Earth and Environmental Science*
[18] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, 2016, pp. 1-3.
[19] G. Prisco (2016, April), The Blockchain for Healthcare: Gem Launches Gem Health Network With Philips Blockchain Lab, [Online]. See at: https://bit.ly/2MQdMHi
[20] O. Williams-Grut (2016, March), Estonia is using the technology behind bitcoin to secure 1 million health records, [Online]. See at: https://bit.ly/2Ih8m3y
[21] P. B. Nichol (2016, March), Blockchain applications for healthcare, [Online]. See at: https://bit.ly/2RiCOgy
[22] Hoang Tam Vo, Lenin Mehedy, Mukesh Mohania, Ermyas Abebe, Blockchain-based Data Management and Analytics for Micro-insurance Applications, CIKM'17, November 6-10, 2017, Singapore
[23] World Health Organization, "Growing threat from counterfeit medicines," Bulletin of the World Health Organization, vol. 88, no.4, pp. 241-320, April 2010.
[24] P. Taylor (2016, April), Applying blockchain technology to medicine traceability, [Online]. See at: https://bit.ly/2XNudoT
[25] Q. K. Nguyen, "Blockchain - A Financial Technology for Future Sustainable Development," 2016 3rd International Conference on Green Technology and Sustainable Development (GTSD), Kaohsiung, 2016, pp. 51-54.
[26] H. Hou, "The Application of Blockchain Technology in E-Government in China," 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, 2017, pp. 1-4.
[27] Jean-Pierre Auffret, "Applying blockchain for eGovernment", Online access January 20, 2019, See at: https://bit.ly/2XNDwVD
[28] Ryan Ayers, "How will blockchain transform the education system?" Online access January 20, 2019, See at: https://bit.ly/2WATcv6
[29] Duan, B., Zhong, Y., & Liu, D. (2017). Education Application of Blockchain Technology: Learning Outcome and Meta-Diploma. In 2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS). IEEE.

[30] Chen, G., Xu, B., Lu, M., & Chen, N.-S. (2018). Exploring blockchain technology and its potential applications for education. Smart Learning Environments, 5(1).
[31] Sharples, M., & Domingue, J. (2016). The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. In Adaptive and Adaptable Learning (pp. 490–496). Springer International Publishing.
[32] Matthew B. Hoy (2017) An Introduction to the Blockchain and Its Implications for Libraries and Medicine,Medical Reference Services Quarterly, 36:3, 273-279.
[33] Rajarshi Mitra, "Complete Guide to Big Data and Blockchain", Online access January 20, 2019, See at: https://blockgeeks.com/guides/big-data-and-blockchain/
[34] Diana Maltseva, "How will Blockchain create wild new opportunities in the business world" Online access January 20, 2019, See at: https://bit.ly/2XojYYh
[35] Joe McKendrick, "Blockchain Opportunities Finally Start To Perk Up Beyond Cryptocurrency", Online access January 20, 2019, See at: https://bit.ly/31CvWPV
[36] Sam Mire, "Blockchain For The Sports Industry: 11 Possible Use Cases", Online access January 20, 2019, See at: https://bit.ly/2qNpV1F

Authors Biography

Md. Saef Ullah Miah is a PhD candidate at Universiti Malaysia Pahang (UMP) and he was as an assistant professor in the CS department of American International University-Bangladesh (AIUB). Possessing real life experience of software development, project management currently indulged in to teaching. Completed his Master of Science and Bachelor of Science degree from AIUB. Besides professional life he serves open source projects and have keen interest in changes in the fields of technologies. His research interest is primarily focused on Data and Text Mining, Machine Learning and Knowledge Management.

Mashiour Rahman obtained his Ph.D and M.Sc from Utara University Malaysia and National University of Singapore, respectively. He is an associate professor and Associate Dean at American International University-Bangladesh (AIUB).

Md. Saddam Hossain obtained his Ph.D and M.Sc degree in Computer science from Bangladesh University of Engineering and Technology

(BUET) and University of Trento, Italy, respectively. He is currently serving as an Assistant Professor in the Dept. of Computer Science and Engineering (CSE), United International University, Bangladesh. He is also an active research member of Data Science and Engineering Research Lab (DataLab), BUET. His research interest is mainly focused on social computing, HCI, Data Mining and Machine learning, and Data & knowledge management. He publishes several journal and conference papers in top tier venues.

Aneem Al Ahsan is currently working as a lecturer in American International University Bangladesh (AIUB). He has completed both his bachelor's and master's from AIUB. His research interest includes data mining, machine learning and image processing. He is actively working with various groups for solving real world problem based on his field of interest. Before joining AIUB he served as technical executive in an organization based on digital marketing. His role was to analyze data to understand consumer interaction with different brands and later provide various analytics which helped in creating creative contents for better marketing thus contributing to the organization's development and fame.

CHAPTER TWO

BLOCKCHAIN FOR INTERNET OF THINGS

BIOZID BOSTAMI[1] AND MOHIUDDIN AHMED[2]

[1]Department of Computer Science and Engineering, Islamic University of Technology, Bangladesh
[2]Academic Centre of Cyber Security Excellence, School of Science, Edith Cowan University, Australia

Abstract

Blockchain, a distributed ledger technology which was introduced in the area of cryptocurrency, has now started to gain attention from different areas beyond its own roots, in circa 2014. Blockchain is used to create secure records in real time, which are tamper-proof and encrypted. On the other hand, the IoT enables intercommunication between objects which are embedded with computing devices, allowing them to send and receive data. In theory, by combining these two, technology will create a verifiable and secure way of preserving data originating from heterogeneous sources, such as 'smart machines'. In the area of the internet of things, some major and open challenges remain regarding data privacy and security issues, due to the distributed nature of IoT networks. With blockchain, most of the open issues could be solved. Theoretically, blockchain holds the solution to many of the open issues of the IoT, but there are some challenges as well. In this chapter, we will be presenting a survey of current discoveries based on blockchain and the IoT, addressing different issues. The main contribution of the chapter will be to provide new directions for the IoT and blockchain research. This chapter will be beneficial for graduate students, academicians, and researchers, in the application domain.

Keywords: Architecture, Protocol, Data Security, False Data Injection Attack, IoT Architecture, IoT Security, Network Security, Network Threats. Smart Contract

1. Introduction

The growth of communication technology has a major impact in our lives. Also, the number of electronic devices has increased. Many of our daily tasks are becoming more and more dependent on electronic devices. Also, the interaction with the environment has become digitized. Digital devices help us with information extracted from the surrounding environment. With the aim of establishing better communication between devices and humans, the internet of things paradigm was invented. The internet of things allows devices to sense, actuate, and communicate over the internet. [2] With currently evolving technology, IoT devices are increasing in number, and being used in many sectors of our society. IoT devices are making our daily lives easier by providing different solutions, such as smart grid, smart city, e-health, smart agriculture, smart education, smart industry, etc. The main vision of the IoT is to achieve a world where every device can communicate over the internet. These IoT devices all have common attributes; they generate data, need connectivity for communication, and interact with the environment through sensors and actuators. But they also suffer some limitations, such as low battery life, low resource, limited memory, etc. To support the growth of the IoT, different communication and security protocols are set, and standard methods are created. But, heterogeneity still remains a challenge in the path of the fully-connected world. Moreover, another issue is trust management. For secure communication, data should be immutable and verifiable.

In 2008, a new technology was introduced with the aim of maintaining data reliability over time. The technology allows data to be saved in an immutable state and ensures reliability over a decentralized, potentially untrustworthy, network. The name of the protocol is blockchain. Blockchain allows data to be stored in an immutable state. It also can be used to make secure and verifiable transactions over an unsecured distributed network, in the absence of a centralized verification entity. By integrating blockchain, many of the limitations faced by the IoT will be solved. But in the practical area, there are some challenges to overcome. These challenges, which are the main contribution of this chapter, can be summarized as follows:

- Study the referential architecture of the IoT infrastructure;
- Study the security issues associated with the IoT network;
- Explore the advantages of blockchain integration with the IoT;
- Explore the open challenges;
- Explore the current blockchain-based applications.

2. The Architecture of the IoT

By the end of 2020, about 25 billion devices for data analysis and autonomous decision-making will be used to communicate through the internet. [1] The IoT is also noted as one of the six 'Disruptive Civil Technologies' by US NIC. We can also see that different sectors, such as smart grid, e-governance, smart health, smart education, smart agriculture, and autonomous business process and manufacturing, etc., have integrated the various architectures of IoT systems. The architecture of the IoT consists of combinations of sensors, actuators, network layers, application layers, IoT protocols, service layers, etc. An ideal IoT system architecture can be seen in Fig 1. The components are described in the following section.

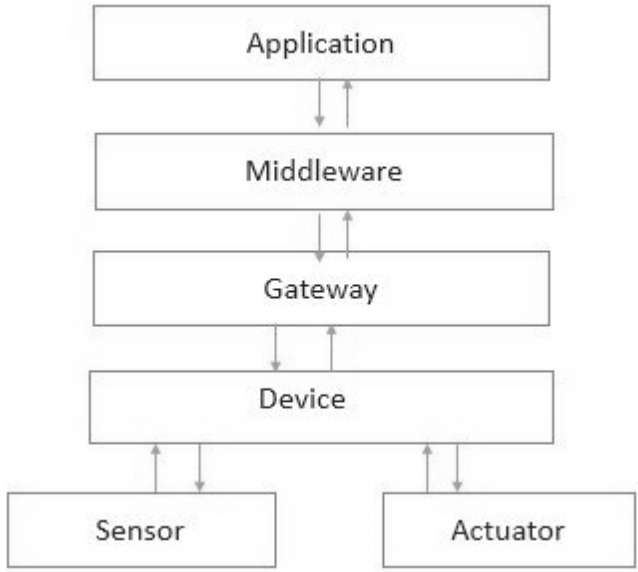


Fig 1: Reference Architecture of IoT System

- **Sensors:** Sensors are core hardware components of the IoT which are used for capturing or monitoring data from the surrounding environment by responding to any changes, such as heat, light, sound, pressure, humidity, etc. Sensors are only sensitive to the phenomenon which they measure. They do not alter the measured data while measuring. There are different kinds of sensor which are used in daily life, such as pressure, heat, light, motion, or gas sensors, etc. For instance, a heat sensor can detect changes in temperature around it. Sensors are used to collect data and transmit them to other electronic devices in the form of electronic signals. The transmission of data from a sensor to other electronic devices can be done in two ways: 1) wired transmission; and 2) wireless transmission. In the case of wired transmission, the sensors are embedded within the electronic devices. Sensors are configurable using other software, but cannot run other software.

- **Actuator:** An actuator is a core component which helps to alter the surrounding environment. IoT devices use sensors, which are used for gathering data from the surrounding environment, but they use actuators to alter events. The actuator acts according to the command it receives from a connected device, in the form of electronic signals or waves. Without actuators, IoT devices cannot make any direct change on their own. For example, an actuator can open or close ventilation, based on the temperature of a room, thus altering the room's temperature. Similar to a sensor, connection between an actuator and a device can be made in two ways: 1) wired; and 2) wireless. Again, actuators cannot configure other software but can be configured by it. Actuators are similar to sensors, only their mechanism is different.

- **Device:** A device is a connector between a sensor and an actuator. The connection can be wired or wireless. Sometimes, sensors and actuators are integrated with a device itself. Unlike sensors and actuators, devices have processors and storage of their own, and can run software and process data. Devices can create connections to the IoT integration middleware. Devices are like a gateway to the digital world from the physical world. They can run different software, generally known as a driver, and help to communicate with a variety of sensors and actuators. Devices can communicate with each other, or share data. Devices can be self-contained, or

they can be a part of a larger IoT system, such as IoT integration middleware, which will be explored later.

- **Gateway:** A gateway is an optional component in IoT architecture. Where the IoT devices cannot directly communicate with remote systems over the internet or middleware, they use a gateway to communicate. A gateway is responsible for maintaining communication between a device and higher systems, such as cloud services or IoT integration middleware. A gateway is used when the device and middleware services use different communication protocols and formats. For example, binary formatted data collected by device sensors may be translated to JSON format before broadcasting to middleware.

- **IoT integration middleware:** This layer is responsible for aggregating different sensors, devices, actuators, and applications. Some of the general responsibilities of this middleware layer are: 1) collecting data from heterogeneous sources**;** 2) processing the collected data; 3) exporting data to the connected applications; and 4) sending commands to devices and actuators based on condition-actions rules. A device supported by proper communication protocols, such as TCP/IP, Bluetooth, Wi-Fi, 4G/5G, LTE, ZigBee, etc., and also corresponding transportation protocols like MQTT or HTTP, and compatible payload formats such as JSON or XML, can directly communicate with the middleware. If not, then the device establishes such communication over the gateway. The responsibility of integration middleware is not limited to those described above. Middleware also handles context detection, device abstraction, and center control management, and also works as an application abstraction, etc. Some middleware supports database and utility features, such as graphical dashboards. Normally, this middleware provides interfaces for high level applications and end-users, providing HTTP APIs methods, like RESTful or SOAP.

3. Security Issues of the IoT

The IoT paradigm consists of a large variety of devices. These devices range from small sensors to large scale servers. That is why security is a big issue. In this section, we will categorize the security issues addressed by different researchers. Based on architecture, we can divide the issues into following categories: [4]

3.1. Physical Layer Security Issues

Low level security issues are concerned with hardware level issues as well as data layer issues. The following section will present a brief idea of the issues related to the physical layer, and solutions proposed by different researchers. [4]

- **Jamming attack**: Jamming attacks are carried out by emitting radio frequencies which target a wireless network, causing deterioration in that target network. [15],[4] This radio frequency interference hinders the regular transmission of data in the network, can cause data loss, and sometimes causes unpredictable behavior among legitimate nodes. Such attacks flood the networks with redundant data, causing message collision. Young et al. [19] proposed a detection method which extracts the adversarial signals based on signal strength, and uses customized thresholds to detect jamming. In their work, Xu et al. [22] show a method based on signal strength and delivery ratio. Their proposed method checks the consistency of the network signal and the node location of the nodes for detecting jamming attacks. Noubir et al. [11] proposed a method to prevent jamming attacks based on cryptographic function and error code correction methods. The proposed method inserts encoded packets of bits in the transmitted packets. Another approach to cope with jamming attacks, based on frequency shifting and spatial retreats, was proposed by Xu et al. [11]

- **Insecure initialization and physical interface:** Initial installation and configuration is the key to ensuring proper service of the system. Proper configuration also increases data privacy and ensures uninterrupted data service. [16],[23] Moreover, physical layer communication should be well secured to prevent unauthorized access. Again, poor physical security and open/less secure access to the software interface, for test and debugging ports, can be easily exploited. In order to prevent unauthorized access, the testing and debugging tools and ports should be disabled. For securing physical layer communication, Pecorella et al. [12] in their work, suggested limiting the data rate between nodes to establish a secure initialization of IoT devices from eavesdroppers. Other approaches for securing physical layer communication include the introduction of artificial noise, which was suggested in [17, 24]

- **Sybil attacks:** Sybil attacks are carried out by nodes which have false identities, but act as valid nodes of a system. [29] These malicious nodes are known as Sybil nodes. These Sybil nodes can generate false reports, and degrade the whole system performance. Sometimes, they prevent legal nodes from gaining access to resources by forging MAC addresses and registering on the system. Demirbas et al. [13] proposed a way of detecting a Sybil attack by deploying detector nodes for communication. These detector nodes are responsible for managing the legal sender nodes. The presence of more sender nodes from the same location triggers the Sybil attack. But the approach can only be valid for static networks. Xiao et al. [5] presented another approach to detecting Sybil attacks, based on different channel parameters and the number of entities in the network.

- **Sleep deprivation attack:** Stajano was the first to come up with the idea of sleep deprivation threat. [6] [14] Most energy-constrained IoT devices are vulnerable to sleep deprivation. These attacks force sensing nodes to remain awake, draining their battery life faster. In order to prevent sleep deprivation attacks on the wireless sensor networks, a different clustering algorithm is suggested by researchers, [18] [20] [21] [25] where a cluster head is set up to be responsible for managing sleep time and patterns of other nodes. But these approaches have one assumption in common, that only valid nodes will participate in the selection processes of cluster heads.

3.2. Network Layer Security Issues

These are the security issues connected with session management, routing, etc., related to the network layer. In the following, we will be exploring some of the issues relating to the network layer, and solutions proposed by the researchers. The following section will only present a brief idea of some solutions proposed by different researchers. [4]

- **Replay attack:** Devices which transmit data packets following IEEE 802.15.4 standards, use fragmentation, where large data is segmented into smaller-size frames. The receiver nodes reconstruct the data by assembling the frames at the network layer. But, devices with 6LowPAN stack may suffer various problems, such as buffer overflow or rebooting, causing data loss. [26] The replay

attacks are carried out by malicious nodes, which send duplicate fragments which hinder the packet re-assembling process, causing loss of data sent by the valid nodes. Kim et al. (2008) introduce nonces and time stamps to address the replay attacks. [26] The time stamps and nonces are added to packet fragments while transmitting. The time stamp reduces redundant packet flooding and redirection within the network. The introduction of a nonce ensures that a request is validated only once. Another option, using a content-chaining method for fragment transmission in 6LowPAN, enabling ordering of fragments, was introduced by Kim et al. [30]

- **Peer discovery:** In a distributed network such as the IoT, devices communicate with each other, and every device is uniquely identified. In order to communicate, devices must discover their peers, and secure peer discovery is a vital issue from the security perspective. The peer discovery stage includes discovery of router links and address resolution. Insecure peer discovery of data packets may cause vital security breaches in the IoT network. For secure peer discovery, Riaz et al. [27] proposed using elliptic curve cryptography (ECC) for key generation and data encryption. The ECC key is used to validate peers during the discovery phase, and ensure secure peer-to-peer data transmission.

- **Sinkhole and wormhole attack:** Sinkhole belongs to the class of insider attacks. Here, a compromised node acts as an attacker which tries to attract all the network requests through the compromised node. Such a node may have carried out different attacks on the network. Another insider attack type is a wormhole attack, where a compromised node transmits the data to another, usually unsecure, location, through a tunnel, and responds back through the malicious node. Such an attack causes privacy violation, security breaches, etc. Many approaches are proposed based on intrusion detection, and pre-defined rules can be found at [7] [28] [31] [32] these rule-based approaches consider network energy, node location, etc. For wormhole attacks, different approaches are also proposed, based on network topology, [33] [35] and key management. [36] Pirzada et al. [37] used dynamic source routing for detecting sinkhole and wormhole attacks. Their approach depends on integrity checks on the forwarding packets.

3.3. Transport Layer Security Issues

The transport layer handles the authentication mechanism and secure end-to-end connection. In the following section, we will be exploring security issues with the transport layer. [4]

- **Authentication issue:** In the IoT system, users and devices need a proper authentication system for ensuring data privacy and integrity. Any loophole in the authentication system may lead to undesirable results. Also, due to resource constraints of IoT devices, cryptographic approaches need careful consideration. Granjal et al. [38] proposed using compressed authentication headers and encrypted payloads. Compressed headers are used either in tunnel mode or transport mode, depending on the payload encryption technique. In their work, they showed that using an SHA algorithm for encryption consumes less time and resource. A similar approach was proposed by Raza et al. [39] using IPsec. In their work, they use NHC encoding for payload encryption, but their approach consumes a lot of resource, which is considered to be a major drawback.

- **End-to-end connection:** In the transport layer secure connection between the source and destination, nodes aim to transfer data in a secure manner, maintaining data privacy. This also requires less overhead, and the data packets are sent across the network in an encrypted form. The secure communication is generally done by two-way key authentication using cryptographic keys. A similar approach was suggested by Kothmayr et al., [40] who proposed to set up an access control server which saves the access rights of all the publishers in the network. Other approaches include passwords and smart cards for authentication and authorization. [41]

- **Session management and resumption:** In the transport layer, a DoS attack can be made by session hijacking and message forging, where the attacking node acts like a valid node, and continues a session which was established with the victim node. The hijacked session continues to exchange messages. The valid messages packets can be sent repeatedly, altering the packet sequence. To counter such an attack, Park et al. [42] proposed a mutual authentication mechanism where the nodes generate a random number, then encrypt the key and generate a session key, which, in

turn, is used to encrypt another generated random number. Then, the final number after encryption is the key for authentication of the session between two valid nodes. With each new session, a new key is generated. To prevent session hijacking in the fog computing servers, and for resource-constrained devices, a similar approach of mutual authentication was suggested by Ibrahim et al. [45] they presented a long-life secret key for session establishment, and named their proposal Octopus.

Threat/Issue	Effects	Layer	Proposed Solutions	Reference
Jamming attack	Network deterioration	Physical layer	Customizing threshold based on signal strength, signal and delivery ratio, error code encryption and frequency shifting	[19,22, 11]
Insecure initialization	Network deterioration, data privacy	Physical Layer	Limiting data rate, adding artificial noise	[12, 17, 24]
Insecure physical interface	Network deterioration	Device hardware	Secure software access open ports, avoiding insecure tools for debugging	
Sybil attacks	Network deterioration, privacy violation	Physical layer	Deploying detector nodes, combination of network parameters	[5,13,29]
Sleep deprivation	Consuming energy	Data link layer	Clustering the network nodes and appointing head nodes	[18, 20, 21, 25]
Replay attack	Network deterioration	Network layer	Using nonce and timestamp for detection, chaining fragment transmission	[26, 30]
Peer discovery	Data privacy violation	Network layer	ECC cryptography to protect data	[27]
Sinkhole and wormhole attack	Network deterioration, privacy Issue	Network layer	Intrusion detection, key management, dynamic source routing	[7, 28, 31, 32, 33, 35, 36, 37]
Authentication issue	Network deterioration, privacy Issue	Transport layer	Compressed header and encrypted payload, SHA algorithm, NHC encoding	[38, 39]
End-to-end communication	Privacy violation	Transport layer	Authentication with cryptic key, smart card, password	[40, 41]

Session management and resumption	Privacy violation, network deterioration	Transport layer	Mutual authentication mechanism with long lived session key	[42,45]

Table1: Summary of security threats and their proposed solutions. [4]

3.4. Application Layer Issues

The application layer security issues are related to the applications which are connected to the application interface and firmware. In the following section, a brief summary of the application layer issues is discussed.

- **Insurance interface:** There can be several interfaces, such as mobile, web, or cloud, for getting access to IoT devices. Such insurance interfaces can be used to violate data privacy, and different attacks can be carried out to disrupt devices' functionality. In order to tackle such issues, there should be limited access to such interfaces, and moreover, only authorized entities should be allowed to make changes.

- **Insecure firmware:** Another major vulnerability in the application layer is insecure software. If there are any bugs or errors in the software code, then the performance of the network will degrade. Again, an attacker may inject malicious codes and compromise the device to carry out further attacks. In order to tackle such cases, the updates or patches of the program should be tested, and secure access control should be deployed to update the firmware securely.

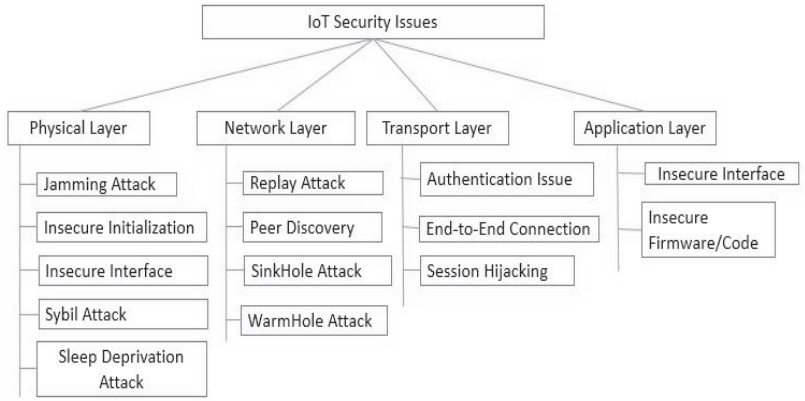


Fig 2: Security issues at different layers of the IoT

4. IoT Security with Blockchain

Blockchain technology has been gaining popularity among researchers and the industrial community, for securing data in a tamper-proof manner, in real time, without the help of any central entity. It is anticipated that blockchain can be used to manage and control IoT devices in a protected environment, since trust is vital where sensitive data is concerned. In the following sections, first a brief summary about blockchain technology is presented, and then there is a brief description of some the key points where blockchain can contribute to security issues with the IoT network.

Blockchain technology was founded in 2008 by Satoshi Nakamoto, in the context of cryptocurrency. In this paper, two new concepts were introduced: 1) Bitcoin; and 2) Blockchain. Bitcoin is a virtual cryptocurrency. The value of bitcoin is not managed or controlled by any centralized financial entity. Rather, bitcoin is securely held in a decentralized P2P network, with unsecured actors who collectively act as a valid and trusted authority. The second concept is blockchain technology, which has gained much more popularity.

Blockchain is basically, a virtual, decentralized, shared, distributed, database ledger, which holds the records of different transactions made across a peer-to-peer network in an immutable state. It provides a secure, tamper-proof, transparent ledger, which can be verified by any entity. All the information relating to transactions, starting from the very first, is

maintained in a structured way, which is known as a block, and each block of transactions is referenced by its previous transaction block. The transactions create a chain of blocks; thus, the name of the mechanism is blockchain. To implement blockchain, the peers in the network must participate and provide functionalities, such as routing, wallet service, mining, and storage, etc. The nodes in the network contribute by providing different functionalities. The routing service is responsible for participation, distribution, and propagation of transaction blocks across the network. The storage service is provided to keep copies of the entire chain, or the part of the chain, in the nodes. The wallet service is used by new transactions. The proof of work is complex, and needs high computational power to publish a block in the network. To publish a block, the proof of work is first done by the miner, and then the block is broadcast in the network, where others also verify the block before adding it to their chain. Since blocks can be generated concurrently, multiple versions of blockchain can exist at a point of time, but to resolve an issue, only the longest version of the blockchain is considered to be valid. Because of the complex proof work in block generation, an attacker cannot alter any block, because even if the attacker does change the block, other valid nodes would have already added new blocks in the network, and thus invalidated the false blocks created by the attacker. In theory, if an attacker can gain 51% of the network resource, it can outperform other miners and create invalid blocks. But this is practically impossible. So, if most the participants are honest then the network will reach a valid state.

Blockchain also introduced a new term, known as ‘smart contract’. Basically, smart contracts are protocols or programs which follow some predefined set of rules while acting as a node in the blockchain network. Smart contracts run some application logic on the transactions made by the participants. Smart contracts replace the need for a trusted third party in the decentralized system of blockchain. For example, a smart contract can set up some application rules which need to be satisfied in order for a transaction to be made. Smart contracts can be programmed to handle different scenarios, other than monetary transactions. Through the use of smart contracts, blockchain can be implemented in other areas. The very first use of smart contracts was first introduced by Ethereum. [44] At present, there are many other uses for the smart contracts, such as Hyperledger, IBM, Intel, etc. A detailed survey on blockchain was presented in [46] Fig 3 shows the basic design of a single block.

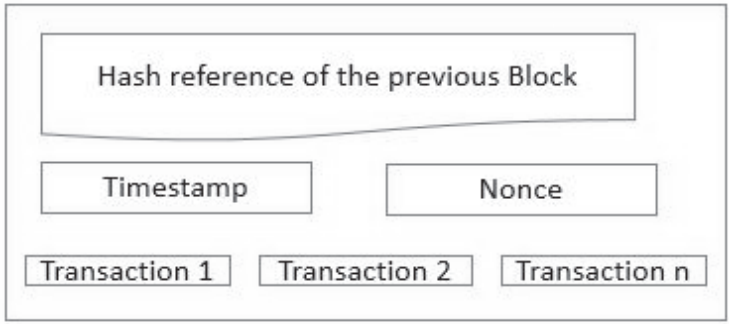


Fig 3: Basic architecture of a block in blockchain

4.1. Improvements of the IoT brought about by blockchain

Blockchain technology is a promising technology for decentralized and trust-based networks, such as the IoT, which demands security and traceability. Blockchain technology ensures that the data in the network remain unchanged, and can be audited at any time. For example, in the case of healthcare or food production platforms, any data leak can cause huge damage to life. Moreover, smart city and smart grids need proper security, or there can be huge economic loss. That is why blockchain is proposed as a solution to data privacy and security in the IoT paradigm. To our best of knowledge, we can say that blockchain can help the advancement of the IoT domain in the future. There are still a lot of open challenges while integrating the two technologies together, which are discussed later. In this section, we will present some of the improvements which can be ensured by the integration of blockchain and the IoT.

- **Decentralized architecture and scalability:** With the integration of blockchain, shifting from a centralized P2P network to a decentralized network can bring some advantages, such as avoiding central failure points and bottleneck attacks. Another advantage of a decentralized network is the increase in fault tolerance and scalability. Again, the control over the network will not belong to any central system or entity. Such decentralized systems design will benefit the IoT system in future.

- **Identity and governance:** Identity management is one of the major challenges for IoT devices. Identity issues include ownership, relationships, and trust. In the case of IoT devices,

ownership can be changed frequently. Again, a relationship between the devices is also required. The IoT relationship can be of various types, such as device-to-device, device-to-human, or device-to-service. The relationship can be changed at any moment. To tackle such situations, the IoT requires trust-based identity management. Blockchain offers a secure and manageable solution for this identity management for IoT devices. Solutions such as Trustchain [34] can provide such an environment, where IoT devices can maintain trusted transactions within the distributed network. Blockchain allows devices to register and gives them identity. Also, IoT devices can be revoked or re-installed with the help of blockchain. Blockchain can track the full life cycle of a connected IoT device, and all the transactions, which solves the issue of IoT device identity management very easily and securely.

- **Address space:** Unlike the IPV6 address space, which is 128-bit, blockchain provides 160-bit address space. This gives more advantages over the IPV6 protocol. Since blockchain has longer address space, it can provide approximately $1.46 * 10^{[48]}$ offline device addresses. Moreover, in order to avoid address collisions, blockchain uses GUID for setting the ID numbers to the devices.

- **Secure deployment:** With blockchain technology, changes in codes and updates of middleware can be securely pushed to the devices. Since blockchain can save all the data in an immutable state, the manufacturers can deploy updates to all the connected devices securely. Moreover, the change log is also saved.

- **Secure communication:** The IoT communication protocol and routing protocols have many security issues. Some of the issues are addressed in this chapter, and different solutions are also discussed. Most of these solutions require an extra layer of security wrapped around the existing protocols. Again, such solutions are complex to manage, and some are expensive in terms of computational power and memory. With blockchain, secure communication can be simplified, since each device is uniquely identified by GUID and asymmetric key pairing when a device is connected to the blockchain network. Such an approach does not need extra methods, such as PKI certification for hand shaking, or encryption or hashing mechanisms for session management.

- **Privacy and authorization:** Smart contracts can provide authorization based on customized rules and requirements for IoT devices. Smart contract authentication and authorization mechanisms are less complex compared with existing protocols, such as OAuth, OpenID, LWM2M, etc. Again, using smart contract, data privacy can also be ensured. Different rules and application logic can be set in order to ensure data privacy. With smart contracts, a different set of roles can be managed, such as who will update software, who can reset a device, who can change the ownership, etc. In summary, smart contracts provide more control over the data privacy authentication mechanism.

- **Reliability:** One of the major advantages of using blockchain is the immutable data record. If the data remain unchanged over time, then it is easier to verify and audit them. Moreover, sensor data can be made traceable.

- **Service oriented market:** A new ecosystem for data-oriented service can be created with the help of the blockchain-based IoT, where different micro services can be deployed, for example, a micro-payment service, where transactions can be allowed in a trust-free environment. Different services can also be interconnecting, and communicate with each other.

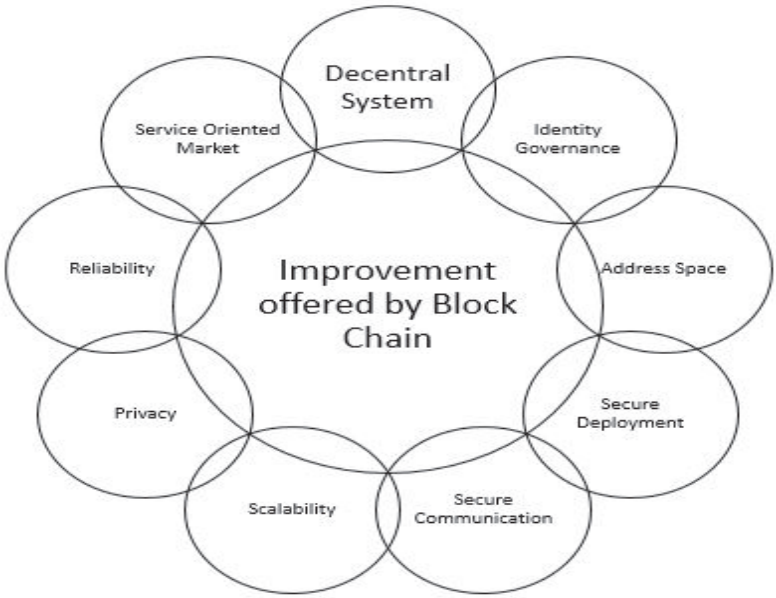


Fig 4: Impact of blockchain in an IoT domain.

5. Infrastructure of Blockchain and IoT Integration

One of the main concerns is the communication between blockchain and the IoT network. The communication can take place between the IoT and blockchain or within the IoT network, or there might be integration with another service, such as fog computing. Based on the data flow and interaction of blockchain and the IoT network, different ways for integration are possible. [3] We will be describing each of these in the following section:

- **IoT-IoT interaction:** In the blockchain-based IoT network, the main interaction will be between the IoT devices. Only partial data will be sent to the blockchain network. In such designs, IoT devices are responsible for device discovery, secure communication, exchange of data, and routing methods. Such an approach is faster while working offline, and such an approach is useful if the IoT devices are ensured as secure by themselves. Figure 5 shows an overview of the system design.

- **IoT-blockchain interaction:** In such a setup, all the transactions are recorded in the blockchain network. Since all the transactions of data are recorded, they are traceable. This also ensures secure communication, and autonomy of IoT devices. Each IoT device is identified by its ID, and blockchain manages access control. Services such as trading, tracking, etc., can benefit from such a setup, but there are some challenges associated with this approach. Since the IoT devices interact through blockchain, this consumes network bandwidth. Again, in order to save all the transactions there must be enough storage. While setting up such an environment, network load and storage facility should be carefully considered.

- **Hybrid approach:** In the hybrid approach, some of the interaction is done between the IoT devices, and some through blockchain. The main challenge is deciding which data should go through the blockchain network. Such an approach has benefits of both IoT and blockchain technology. In this setup, cloud computing and fog computing can play a major role. Fog computing can be connected to IoT devices using a gateway, providing the computational power for mining, encryption, etc. Moreover, for resource-constrained devices, connection with blockchain can become costly, so the cloud can act as middleware for the connection. A hybrid approach is suitable where high optimization is required. One drawback of using a cloud computation is that clouds are designed for centralized systems. This could limit the reliability of the data. But recently, fog computing is designed for distributed nature systems, which could benefit the integration of blockchain and IoT in the future.

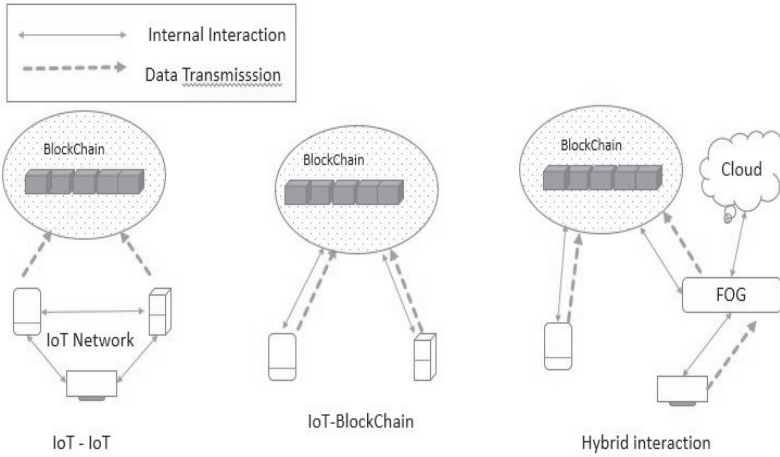


Fig 5: Different ways of IoT and blockchain integration

6. Blockchain-based IoT Applications

Although blockchain technology was initially introduced for cryptocurrency, researchers have proposed that the IoT can heavily benefit from the integration of blockchain technology. Even though the proposal of blockchain-based IoT is very recent, many applications can be found. Here we will provide a brief summary of some the blockchain-based IoT application.

Among all the blockchain-based IoT applications, Ethereum[44] is the most popular. It has more features than bitcoin. Again, smart contracts integration means it can be integrated into all the domains of the IoT.

ADEPT [43] is another example of blockchain-based IoT application. It aims to build a decentralized peer-to-peer telemetry. The whole project is supervised by Samsung and IBM, who use different decentralized technology for file message sharing, such as BitTorrent, Ethereum, and Telhash. Blockchain was used for access control, security, and contract management.

Aigang[52] is a blockchain-based IoT application in the insurance network of IoT assets. This offers insurance to different products with different risk levels. The risk assessment, issuing policy, claims, etc., are automated,

using smart contracts. It also created a new virtual currency, called AIX. Smart contracts allow maintenance calls to be made automatically.

LO3 Energy[51] is the first smart microgrid built on a decentralized P2P network with blockchain integration. The devices at the end points can securely distribute power to the participants in the microgrid. The production of power and distribution data is saved in the blockchain network, and can be used for report and analysis.

Chronicled[50] has developed many products with a view to creating the world first blockchain IoT network for supply chain management. Their aim is to connect different blockchain technologies, such as Ethereum, Hyperledger, etc. The products are cryptographic capabilities, and use smart contracts to register and communicate.

Modum is also a blockchain-based IoT solution, which aims to improve the supply chain process of medicine. The solution is designed to track medicine product distribution. Smart contracts are used to validate transactions. Sensors are used to read the tags and track the items during the shipping process. Using the dashboard, the data can be analyzed once the shipping process is completed.

The twin of things[49] is another blockchain-based IoT solution, aiming to manage the ownership of daily life objects. It was created using Ripple and code. It is a hardware-based solution which is basically a secure crypto chip that transforms any physical object into a node. These nodes have unique identification numbers, and can be connected to the blockchain network. After the device is connected to the blockchain, communication with other connected devices is established. The solution is designed to work with various blockchain applications, such as bitcoin, Ethereum, etc.

The Chain of Things,[48] is a blockchain-based research lab which provides various blockchain-based IoT solutions. One of their recent applications is an identity management system, named Blockpass, which can be used for the identification of humans, devices, or objects. Such applications can be used for environments which rely on multiple entities. The Chain of Things also presented three case studies: the Chain of Security, which aims to provide security among IoT devices; the Chain of Solar, which aims to provide blockchain-based solar panel solutions for energy production; and the Chain of Shipping, aiming to tackle the security faults in the supply and logistics industry.

IoTex[47] is also based on blockchain and the internet of things, providing privacy-preservation solutions for decentralized distributed enterprise applications. It is highly scalable, and also provides cross-chain communication.

7. Open Challenges in Blockchain-based IoT

Blockchain was initially designed for high computational devices which can handle crypto currency with digital signature. So, integrating such technology with IoT is not a straightforward task. In this section, we will be highlighting some of the open issues which need special attention while integrating blockchain with the internet of things (IoT).

- **Scalability and storage**: The context of scalability and storage of IoT devices has always been a limitation which makes it more challenging for more complex blockchain integration. IoT devices generate a huge of amount of data in real time, but on the other side, blockchain can only handle fewer requests per second, making it a greater challenge to integrate with IoT devices. This problem can be alleviated by saving the necessary part of the collected data. Once data is collected by the sensor nodes, it can be filtered by services such as cloud and blockchain, and only the compressed and important data needs to be saved for later processing. Data compression and filtering can also speed up processing and transmission.

- **Data Privacy:** One of the core issues with IoT devices is the many applications of the IoT which deal with confidential data. Blockchain does support anonymity along with data privacy, but in the context of IoT, there are more aspects to focus on. Within the IoT devices, data is collected and transmitted, through the communication layers to the application layer. Securing the devices from any kind of tampering or unauthorized access is difficult, since this requires integrating different cryptographic software. Different approaches based on SSL, IPsec, etc., may be introduced, but devices have limited resources, and these are not economically viable.

- **False data injection:** Another open challenge in the domain of the internet of things and blockchain is false data injection attacks. IoT devices can generate false data, for many reasons, such as incorrect

installation**,** hardware damage, network failure, etc. Again, malicious users may inject false data by tampering with the hardware, sacrificing nodes, or bypassing the security layers which are addressed in Bostami, Ahmed, Choudhury (2019) "False Data Injection Attacks in Internet of Things". [53] The false data injection attacks have been heavily studied for smart grid systems, but other areas of the IoT are still vulnerable to such attacks. Since the blockchain data is immutable, it creates a challenge on how to handle the corrupt data once it is fed to the system. Such cases need special attention in the case of blockchain-based IoT.

- **Smart contracts:** Smart contracts are a popular application in blockchain. But there are issues which need to be considered while integrating blockchain and the IoT domain. A contract resides in a specific blockchain address, which listens to different events, via public functions, called up by the IoT devices. These functions can also trigger events to the devices, and they act accordingly. The contracts save the different states. Whenever a state is changed, due to an event, a transaction is broadcasted. The states are changed when the network approves the transaction. IoT devices sense and act with the environment, based on events, so smart contracts can save all the event change records properly. Smart contracts demand the use of special entities, known as oracles, for providing data in ensuring security. But the IoT devices can be easily compromised, and heterogeneous data sources create an extra load for smart contracts. While integrating IoT with blockchain, smart contracts need to address the heterogenic nature of the IoT. Again, for faster response, new methods of actuation are also required.

- **Legal issues:** Within the law relating to data privacy, protection is an open challenge, since these laws are not yet fixed. Moreover, in the case of blockchain-based technology, key resetting or revision of an earlier transaction is not possible. Moreover, the law regarding how a blockchain-based centralized system will be managed is still a question. For example, the centralized system may manage the whole network like a county, or the whole network could be open for all. These laws will determine the future of blockchain and the IoT system.

- **Consensus**: Another open challenge in the way of blockchain integration is the consensus mechanism, since most IoT devices

have limited resources, which makes them unsuitable for consensus mechanisms, such as proof of work (PoW). There are many other consensus mechanisms suggested by different researchers, but they have not been tested sufficiently for real world application. Again, the consensus mechanisms require huge processing power, so new consensus techniques, with the focus on less power and resource consumption, are needed, and this remains an open challenge yet to be tackled.

8. Conclusion

As with any other disruptive technology, blockchain has also created a lot of controversy. Even though it was invented for cryptocurrency, it has now proved that it has its own potential to be used in other domains. Integration with the IoT domain can bring about revolutionized change. Many of the drawbacks of IoT can be solved using blockchain integration. Even though blockchain is said to be the key to many problems associated with IoT security, there are still some unsolved challenges which need to be addressed by the researchers' community. Here we have tried to present the basic structures of IoT and its different security issues. Also, we have highlighted the way blockchain can address these issues, and presented some of the recent applications of blockchain-based IoT applications. The main aim was to show the fact that the integration of IoT and blockchain will benefit both technologies. Different limitations of the IoT will be solved, and many more applications will be created, using blockchain technology. Lastly, there is still a lot of research to be done on both the technologies regarding security and scalability.

References

[1] J. Rivera, R. van der Meulen, Forecast alert: internet of things — endpoints and associated services, worldwide, 2016, Gartner (2016).
[2] M. Díaz, C. Martín, B. Rubio, State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing, J. Netw. Comput. Appl. 67 (2016) 99–117.
[3] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz, On blockchain and its integration with IoT. Challenges and opportunities, Future Generation Computer Systems, Volume 88,2018, Pages 173-190,ISSN 0167-739X, https://doi.org/10.1016/j.future.2018.05.046.

[4] Minhaj Ahmad Khan, Khaled Salah,IoT security: Review, blockchain solutions, and open challenges,Future Generation Computer Systems, Volume 82,2018,Pages 395-411, ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.11.022.
[5] L. Xiao, L. J. Greenstein, N. B. Mandayam, W. Trappe, Channel-based detection of sybil attacks in wireless networks, IEEE Transactions on Information Forensics and Security 4 (3) (2009) 492–503.
[6] F. Stajano, Security for Ubiquitous Computing. John Wiley & Sons, Ltd., 2002.
[7] Krontiris, I. Dimitrou, T. Freiling, F.C. (2007). Towards intrusion detection in wireless sensor networks. In Proc. Of the 13th European Wireless Conference.
[10] W. Xu, T. Wood, W. Trappe, Y. Zhang, Channel surfing and spatial retreats: Defenses against wireless denial of service, in: Proceedings of the 3rd ACM Workshop on Wireless Security, WiSe '04, ACM, New York, NY, USA, 2004, pp. 80–89. doi:10.1145/1023646.1023661.URL http://doi.acm.org/10.1145/1023646.1023661
[11] G. Noubir, G. Lin, Low-power dos attacks in data wireless lans and countermeasures, SIGMOBILE Mob. Comput.Commun. Rev. 7 (3) (2003) 29–30.
[12] T. Pecorella, L. Brilli, L. Muchhi, The role of physical layer security in iot: A novel perspective, Information 7 (3).
[13] M. Demirbas, Y. Song, An rssi-based scheme for sybil attack detection in wireless sensor networks, in: Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, WOWMOM '06, IEEE Computer Society, Washington, DC, USA, 2006, pp. 564–570. doi:10.1109/WOWMOM.2006.27. URLhttp://dx.doi.org/10.1109/WOWMOM.2006.27
[14] F. Stajano and R. Anderson, "The resurrecting duckling: security issues in ad-hoc wireless networks," in Proc. of the Third AT&T software symposium, 1999.
[15] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc '05, ACM, New York, NY, USA, 2005, pp. 46–57. doi:10.1145/1062689.1062697. URL http://doi.acm.org/10.1145/1062689.1062697
[16] Y.-W. P. Hong, P.-C. Lan, C.-C. J. Kuo, Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal

processing approaches, IEEE Signal Processing Magazine 30 (5) (2013) 29–40.
[17] S. H. Chae, W. Choi, J. H. Lee, T. Q. S. Quek, Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone, Trans. Info. For. Sec. 9 (10) (2014) 1617–1628. doi:10.1109/TIFS.2014.2341453.URL http://dx.doi.org/10.1109/TIFS.2014.2341453
[18] S. Bandyopadhyay and E. J. Coyle, "An energy-efficient hierarchical clustering algorithm for wireless sensor networks," in INFOCOM, vol. 3, 2003, pp. 1713–1723.
[19] M. Young, R. Boutaba, Overcoming adversaries in sensor networks: A survey of theoretical models and algorithmic approaches for tolerating malicious interference, IEEE Communications Surveys Tutorials 13 (4) (2011) 617–641. doi:10.1109/SURV.2011.041311.00156.
[20] T. Bhattasali, R. Chaki, A Survey of Recent Intrusion Detection Systems for Wireless Sensor Network, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011, pp. 268–280
[21] E. J. Duarte-Melo and M. Liu, "Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks," in Globecom, 2002, pp. 21–25.
[22] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc '05, ACM, New York, NY, USA, 2005, pp. 46–57. doi:10.1145/1062689.1062697. URL http://doi.acm.org/10.1145/1062689.1062697
[23] S. H. Chae, W. Choi, J. H. Lee, T. Q. S. Quek, Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone, Trans. Info. For. Sec. 9 (10) (2014) 1617–1628. doi:10.1109/TIFS.2014.2341453. URL http://dx.doi.org/10.1109/TIFS.2014.2341453
[24] Y.-W. P. Hong, P.-C. Lan, C.-C. J. Kuo, Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches, IEEE Signal Processing Magazine 30 (5) (2013) 29–40.
[25] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in HICSS, 2000.

[26] H. Kim, Protection against packet fragmentation attacks at 6lowpan adaptation layer, in: 2008 International Conference on Convergence and Hybrid Information Technology, 2008, pp. 796–801. doi:10.1109/ICHIT.2008.261.

[27] R. Riaz, K.-H. Kim, H. F. Ahmed, Security analysis survey and framework design for ip connected lowpans, in: 2009 International Symposium on Autonomous Decentralized Systems, 2009, pp. 1–6. doi:10.1109/ISADS.2009.5207373.

[28] Krontiris, I., Giannetsos, T. and Dimitriou, T. (2008). Launch Sinkhole Attack in Wireless Sensor Network; the Intruder Side. In Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing, (pp. 526-531). IEEE.

[29] L. Xiao, L. J. Greenstein, N. B. Mandayam, W. Trappe, Channel-based detection of sybil attacks in wireless networks, IEEE Transactions on Information Forensics and Security 4 (3) (2009) 492–503.

[30] H. Kim, Protection against packet fragmentation attacks at 6lowpan adaptation layer, in: 2008 International Conference on Convergence and Hybrid Information Technology, 2008, pp. 796–801. doi:10.1109/ICHIT.2008.261.

[31] Tumrongwittaya and Varakulsiripunth. (2009). Detection of Sinkhole attack in Wireless Sensor Networks, In ICCAS-SICE, 2009 (pp. 1966-1971). IEEE

[32] Choi, G. B., Cho, J. E., Kim,H. J., Hong, S. C. and Kim, H. J. (2008).A sinkhole attack detection mechanism for LQI based mesh routing in WSN. In ICOIN (pp.1-5).

[33] Radha Poovendran and Loukas Lazos. A Graph Theoretic Framework for Preventing the Wormhole Attack in Wireless Ad Hoc Networks. ACM Wireless Networks (WINET).

[34] P. Otte, M. de Vos, J. Pouwelse, Trustchain: A sybil-resistant scalable blockchain, Future Generation Computer Systems. doi:https://doi.org/10.1016/j.future.2017.08.048. URL http://www.sciencedirect.com/science/article/pii/S0167739X17318988

[35] Weichao Wang and Bharat Bhargava. Visualization of Wormholes in Sensor Networks. In Proceedings of ACM Workshop on Wireless Security (WiSe 2004), October 2004.

[36] J. Jang, T. Kwon, J. Song, A time-based key management protocol for wireless sensor networks, in: Proceedings of the 3rd International Conference on Information Security Practice and Experience, ISPEC'07, Springer-Verlag, Berlin, Heidelberg, 2007, pp. 314–328.

[37] A. A. Pirzada, C. McDonald, Circumventing sinkholes and wormholes in wireless sensor networks, in: International Workshop on Wireless Ad-hoc Networks 2005, 2005.
[38] J. Granjal, E. Monteiro, J. S. Silva, Enabling network-layer security on ipv6 wireless sensor networks, in: 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, 2010, pp. 1–6. doi:10.1109/GLOCOM.2010.5684293.
[39] S. Raza, S. Duquennoy, J. Hglund, U. Roedig, T. Voigt, Secure communication for the internet of thingsa comparison of link-layer security and ipsec for 6lowpan, Security and Communication Networks 7 (12) (2014) 2654–2668. doi:10.1002/sec.406
[40] T. Kothmayr, C. Schmitt, W. Hu, M. Brnig, G. Carle, A dtls based end-to-end security architecture for the internet of things with two-way authentication, in: 37th Annual IEEE Conference on Local Computer Networks - Workshops, 2012, pp. 956–963. doi:10.1109/LCNW.2012.6424088.
[41] X. Huang, Y. Xiang, E. Bertino, J. Zhou, L. Xu, Robust multi-factor authentication for fragile communications, IEEE Transactions on Dependable and Secure Computing 11 (6) (2014) 568–581. doi:10.1109/TDSC.2013.2297110.
[42] N. Park, N. Kang, Mutual authentication scheme in secure internet of things technology for comfortable lifestyle, Sensors 6 (1) (2016) 20–20.
[43] P. Veena, S. Panikkar, S. Nair, P. Brody, Empowering the edge-practical insights on a decentralized internet of things, in: Empowering the Edge Practical Insights on a Decentralized Internet of Things, vol. 17, IBM Institute for Business Value, 2015.
[44] V. Buterin, Ethereum white paper, 2013.
[45] M. H. Ibrahim, Octopus: An edge-fog mutual authentication scheme, International Journal of Network Security 18 (6) (2016) 1089–1101
[46] Zheng, Z., Xie, S., Dai, H-N., Chen, X. and Wang, H. (2018) 'Blockchain challenges and opportunities: a survey',Int. J. Web and Grid Services, Vol. 14, No. 4, pp.352–375
[47] IoTex, 2019. Available Online: https://iotex.io/
[48] Chain of things, 2019. Available online: https://www.chainofthings.com
[49] Riddle and Code, 2019. Available online: https://www.riddleandcode.com.
[50] Chronicled, 2019. Available online: https://chronicled.com/.
[51] LO3ENERGY, 2019. Available online: https://lo3energy.com/.

[52] Aigang , 2019. Available online: https://icobench.com/ico/aigang
[53] Bostami B., Ahmed M., Choudhury S. (2019) False Data Injection Attacks in Internet of Things. In: Al-Turjman F. (eds) Performability in Internet of Things. EAI/Springer Innovations in Communication and Computing. Springer, Cham

Authors Biography

Biozid Bostami finished his Bachelor of Science Degree in Computer Science and Information Technology with High Distinction from Islamic University of Technology, OIC. He is working in the area of Big Data Mining, Machine Learning and Network Security in collaboration with Mohiuddin Ahmed. He is working to develop efficient and accurate Anomaly Detection techniques for network traffic analysis to handle the emerging Big Data problems.

Mohiuddin Ahmed attained his PhD in Computer Science from UNSW Australia. His research expertise encompasses cyber security and machine learning, and covers a wide range of application domains. Mohiuddin holds over five years of data science and cyber security experience. He is currently working as a Lecturer in Computing and Security Sciences in the School of Science at Edith Cowan University. Prior to joining ECU, he served as a Lecturer in the Centre for Cyber Security and Games at Canberra Institute of Technology (CIT) and was also involved with CIT's Data Strategy Working Group.

CHAPTER THREE

BLOCKCHAIN AND INDUSTRY 4.0

SABBIR AHMED AND RAZIB HAYAT KHAN

Department of Computer Science, American International University-Bangladesh

Abstract

Industry 4.0 reveals the fourth industrial revolution that includes the internet of things (IoT), cloud computing, cyber-physical systems, and cognitive science. This enables users to perform real-time system interactions with the help of the IoT and cyber-physical systems. This interactive process is supervised by tightly integrated algorithms and software. The physical infrastructures are converted to a virtual network which allows decentralized decision making. If we consider the financial sector, decentralization has become the trending concept. Integration of blockchain comprised of cryptocurrency ensures safety in the digital ledger. Above all, blockchain has sufficient potential to build efficient, flexible, and optimized business models, as well as to ensure the security and trust of all stakeholders. Bearing this concept in mind, we describe in this chapter about how we can enhance the performance of Industry 4.0 by integrating blockchain. The chapter includes the introduction and issues of Industry 4.0, blockchain implementation, utilization, and future business scope to support Industry 4.0.

Keywords*:* Blockchain, cybersecurity, cyber physical system, decentralize process, distributed process, IoT, Industry 4.0, industrial revolution, privacy, smart city, smart product, smart warehouse

1. Introduction

The main objective of Industry 4.0 is to permit rapid advances in industrialization and information dissemination methods for recent technologies. Most businesses are trying to grab the benefits of Industry 4.0. In terms of implementing a fully digitized city, we are moving closer using smart technologies and smart appliances. As industrial systems have entered the cyber-physical sphere, involving real-time communication with hyper-connectivity, new security challenges arise. Due to the development of smart systems with Industry 4.0, concentration has been focused on the security of personal and financial information. On the other hand, to implement a robust communication system with hyper connectivity, a smart approach is needed to protect the hyper-related infrastructure data.

Blockchain technology is generally associated with cryptocurrencies, for example, bitcoin, despite the fact that it has a great deal of other use cases, like cyber-security in Industry 4.0. Furthermore, with the advance of blockchain, we are, as of now, on the pathway to fulfilling the criteria set out by the fourth industrial revolution. As the objectives of Industry 4.0 need to concentrate on protecting individual information and transaction-related data, its identified endeavors and participants have to be monitored all around. Blockchain is considering improvements that will deal with cybersecurity risk management for Industry 4.0. Therefore, blockchain technology has the ability to build an innovative cybersecurity system, providing the assurance of confidentiality of sensitive data. Therefore, although enablement of blockchain is not replacing the technology, nor the system, it can resolve some issues, and also offer some solutions to inherent issues.

The rest of the chapter is organized as follows. The terms and trends which are directly involved with Industry 4.0 are described in section 2. We also present an overview of the problems due to the implementation of Industry 4.0. The challenges associated with security systems have been discussed in section 3. To ensure better security and greater accountability, the ways in which blockchain can be applied for Industry 4.0 are covered by section 4, which also addresses the opportunity of scalability, using the real-time blockchain-based system. An architecture which illustrates how blockchain implementation can create the scope to fulfill the demand of Industry 4.0-based applications is discussed in section 5. We discuss various smart systems and the uses of blockchain in section 6. Advanced blockchain can make changes in Industry 4.0, and can play a huge role in

future business. Section 7 highlights the possible scope and future possibilities of blockchain implementation in Industry 4.0. The chapter concludes with section 8, which also provides a short summary.

2. The Industrial Revolution towards Industry 4.0

The history of industrial revolution is long, and its advances are changing over time, driven mainly by the advancement of technology, and more specifically, by the integration of information technology. The concept of industrial revolution was first introduced in the late 18th century in Europe and the US, where it followed the introduction of water and steam power-based mechanical manufacturing facilities for mass production, described in Figure 1. This is the era of transition towards the use of heavy instruments for production line improvements. At the start of the 19th century, the industrial revolution moved forward to the introduction of electrically-powered mass production, based on division of labor that elevates the standard of living of human civilization. After that period, in around 1970, automation, through the use of electronics and IT, which adds faster and more machine-controlled mass manufacturing processes on the edge of industrial revolution, has become popular. Now, the industrial revolution is fully influenced by cyber-physical systems which introduce the idea of Industry 4.0; the era that reveals the use of the latest development trends in production systems, maintaining a pure equilibrium in the integration of man and machine, to build up an intelligent network. [24]

3. Industry 4.0

Industry 4.0 is the present drift of digitized society due to information exchange and computerization. It helps in the creation and improvement of new technologies. However, this is not a new business structure, it is not even a new technology. Industry 4.0 has digitally improved production lines and turned them into ‘smart’ technologies with the utilization of the internet of things (IoT). It uses physical frameworks, on a virtual system, to perform decentralized decisions. To make real-time interactive systems, it uses cyber-physical systems with IoT.

The technology dimension of Industry 4.0 is using many of the latest automation features in manufacturing and other industry services. Improved performance can be achieved in manufacturing processes through real-time integration and massive data analysis that will further

ensure the optimized use of resources. An overview of the fourth industrial revolution, which involves lots of different technologies and their current trends, is illustrated in Figure 2. The main aspect of Industry 4.0 is an integrated system, and that includes various IoT devices, cloud computing, and big data analysis. The interest in new and more intelligent innovation is expanding exponentially. Organizations are starting to use 3-D printing in modelling and creating singular segments for manufacturing. Robots will, in the long run, figure out how to collaborate with each other, working securely, one next to the other, and gaining from each other.

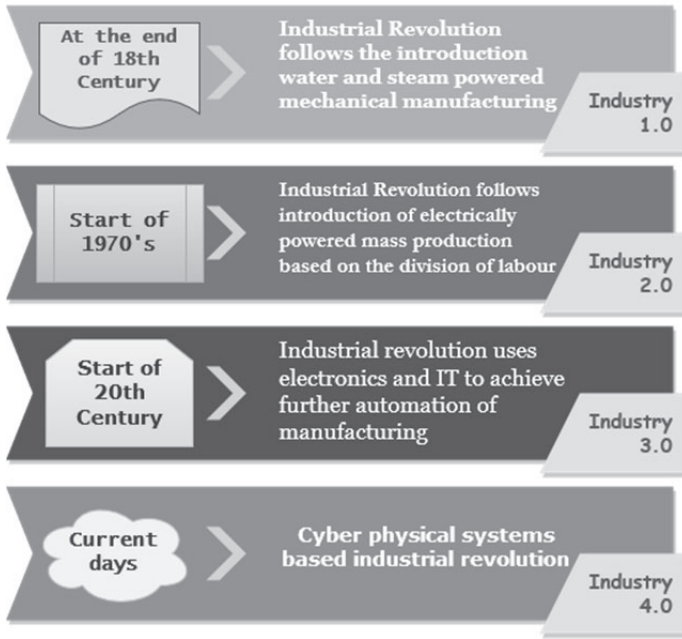


Figure 1: Industry revolutions - four stages

The development of Industry 4. 0 is directly associated with the changes and current intents of IoT technologies. Strong and accurate data and services are provided through the integration of cloud computing and mobile computing, along with industrial IoT networks. In production, a massive number of different data are produced, due to pervasive incorporated information and communication. The productivity and data transparency in big data can be achievable through the monitoring of the smart manufacturing pattern and the industrial big data environment. [13]

Due to a complex cyber-physical system, different kinds of device are equipped with the IoT for sensing, processing, sharing, and communicating capabilities. The life cycle of a product is dynamic in nature (additive manufacturing). Thus, it will be more effective and efficient if the dynamic process is assisted by decentralization, self-optimization, and automation. The IoT provides opportunities to build a decentralized information processing system, to pertain analytics, and to enable real-time responses. The relationships among clients, producers, and suppliers will be improved by the use of the IoT and Industry 4.0. Creating choices won't be overwhelmed by producers and vendors. The IoT and Industry 4.0 will settle for customers continuously going with decisions about the quality and the customization of items. [13] [17] [11]

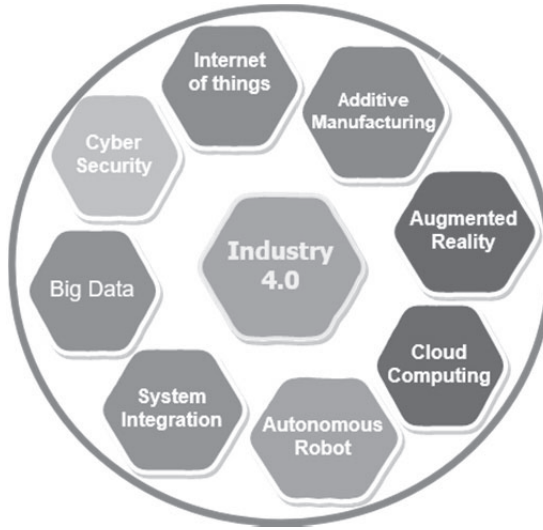


Figure 2: Overview of Industry 4.0

4. Issues of Industry 4.0

Information safety and trust are the primary concerns while considering the interoperability of Industry 4.0. This requires explicit standards to ensure the total procedure of exactness and productivity. For example, an incorporated framework for a savvy city could be interoperable while it can guarantee the accessibility, safety, confidentiality, and utilization of open benchmarks. [13] [1]

Accessibility means equal opportunities should be guaranteed for related participants and should also provide public access without any discrimination.

There are numerous smart applications based on IoT devices in the smart city infrastructure construct. These applications make urban people's lives easier. Apart from its benefits, IoT-based applications have some serious issues. Figure 3 describes a different kind of security issue which comes with the IoT. IoT devices which are available in the market contain several bugs, so hackers may get access to the system through these bugs. They can spill public privacy or even become harmful. So, in recent years, data security and monetary privacy have become increasing concerns amongst all individuals. In order to keep information safe and reliable, necessary policies need to be ensured, which is the main concern in terms of security. Appropriate security measures and risk assessment activities are required.

Privacy means not sharing any data with others, even within an integrated system. In a cyber-physical system, it is necessary to ensure data privacy from IP theft or counterfeiting, and from the cloning of products.

Figure 3: Security challenges of IoT technology in Industry 4.0

Universal standards are required to process any information through cyber-physical systems. In order to fulfill the different requirements of different participants or partners, standard rules and regulations have to be in place. Cybersecurity is an enormous concern, owing to its multifaceted nature and dynamic administration process. However, it is an even more challenging task to produce a secured high-level IoT-based cybersecurity architecture for Industry 4.0. [7] [25]

Generally, due to the advancement of new technologies, there are a lot of operational issues that need to be addressed as a vital concern for Industry 4.0. Because of the advancement of the internet, data security has become a significant concern. There are numerous smart applications in the smart city infrastructure construct based on IoT devices. Figure 4 demonstrates that stakeholders and users are facing the problem of sharing their private information. Businesspeople are very concerned about their confidential business information sharing in the integrated framework due to data privacy. On the other hand, users want a trustworthy system where they can perform secure financial transactions. Users are relying on trusted third party organizations to make transactions. Existing systems need to be integrated with new approaches, and thus it can be a complex affair to deal with integrated systems. Perhaps, it will require slower and even trickier maintenance to make the existing systems fully functional with Industry 4.0 approaches.

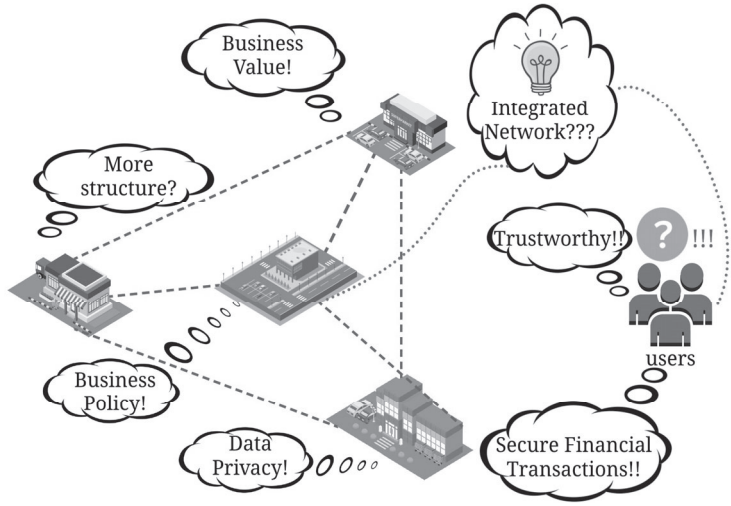


Figure 4: Problems with Industry 4.0 implementation

5. Blockchain: The Backbone of Industry 4.0

In the structure of a smart city, everything should be interconnected through the cyber-physical system. Thus, the integrated system is one of the prime criteria which has ensued from Industry 4.0. The complex, interconnected, multiparty businesses will benefit from the implementation of blockchain. Since, in a smart integrated system, multiparty businesses will be interconnected in cyber-physical space through the internet, peer-to-peer interaction can be dealt with in such a situation. Therefore, all parties will have the transparency of transactions with the involvement of safety and security. A product can be easily traceable, since every record of the manufacturing chain is going to be stored in the digital ledger.[3]

In general, blockchain is a chain of blocks or transactions which is mutually prolonged through the network, by every participating node. The blocks are leashed together cryptographically. Each block is digitally signed and contains the hash value of the previous block. New blocks can only be joined to the end of the chain. So, the prior existing transactions cannot be updated or deleted. This feature makes the blockchain an immutable data storehouse. There are three key aspects of blockchain which are described in Figure 5: smart digital signature, shared or distributed ledger, and consensus cryptographic algorithm. So, we can say that it is a technology which uses the combination of distributed database, cryptography, and a set of consensus algorithms.

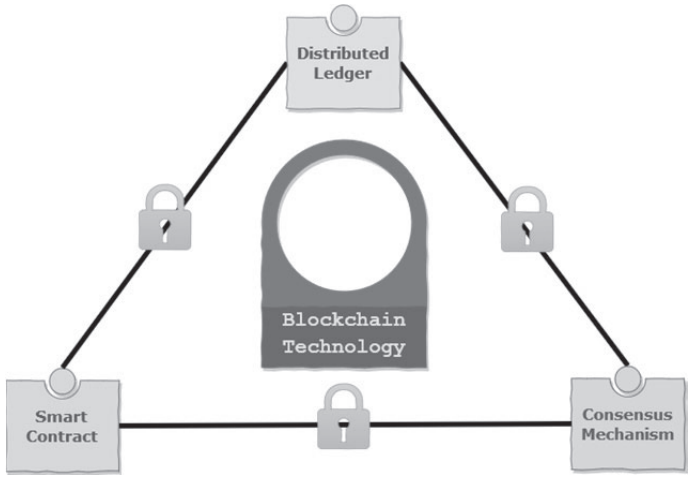


Figure 5: Blockchain architecture

5.1 Better, and Secure, Contract Management and Procurement

Blockchain provides the advantages of improved contract management and acquisition with the help of a smart contract. A smart contract is a computer protocol which is usually used for checking the authenticity of a transaction. This makes the process easier, and secure, by performing digital processing and verifying. It permits each party to make dependable, controlled, and irrevocable, transactions without the inclusion of a trusted outsider for approval. The aim of smart contracts is to provide security and transparency among stakeholders while performing any transactions. When a transaction is done, the distributed ledger is updated, after verifying by the other nodes available in the network. [12] [18]

5.2 Greater accountability ensuring effective quality control

Blockchain maintains its records using an interconnected set of blocks where every block encompasses a list of transactions, a time stamp, and information on the previous and next block. This feature makes blockchain extremely strong, immutable, and free from attacks by any unauthorized person. The ledger is updated every time a transaction is made, and since the ledger is available publicly, the transparency of the system is ensured. Maintaining transparency and privacy in the digital records ensures quality assurance and accountability.

5.3 Blockchain Exhibits New Scope for Scalability

Blockchain brings the benefit of scalability. Blockchain technology offers us a new idea in information collection and distribution. By allowing digital information to be distributed without being copied, blockchain technology creates the backbone of a new type of internet. In general, blockchain is a chain of blocks or transactions which is mutually prolonged by every participating node through the network. In this model, every stakeholder is acting as both server and client. It permits straight data transmission amongst stakeholders. In effect, this feature enables the integration facility among the different multiparty businesses. All stakeholders in a smart city will exchange information in a distributed, but integrated, infrastructure through this network. [18]

5.4 Likely uses of Blockchain in Industry 4.0

Significant impact has been made by blockchain technology in terms of cryptocurrency. Blockchain innovation is commonly associated with digital forms of money, for example, bitcoin. Since blockchain is used in a distributed network, this requires a large number of users to make it more robust.

Blockchain innovation will work in Industry 4.0, considering the fact that it can track the records and confirm the transactions with a proper authentication mechanism. The blockchain is used as the promising candidate in the context of data security and privacy. This technology offers a new idea in information gathering and dissemination, by allowing digital information to be distributed, but not replicated.

6. Blockchain Implementation to Support Industry 4.0

With the integration of cryptocurrencies, blockchain has gained popularity in the financial industry. Though blockchain is used for cryptocurrency, it has the potential to be used in many sectors, where it allows parties to make reliable transactions. Due to the use of blockchain, financial services will work without the involvement of a trusted third party.

The proposed model in Figure 6 illustrates the blockchain-based multiparty integrated infrastructure. In this architecture, blockchain technology secures decentralized information processing, through its consensus mechanism. This mechanism also confirms a copy of the shared ledger in the network carried by each node. The aim of smart contracts is to provide security and transparency amongst stakeholders, to make transactions. When a transaction is made, the distributed ledger is verified by the other nodes present in the network, and is updated. We can also refer to this as an interconnected set of blocks where each block contains a list of transactions, a time stamp, and information about the previous and next block. In every block, a block header also contains the hash of the previous block, along with an arbitrary number. This feature makes blockchain extremely strong, immutable, and invulnerable to attack from any unauthorized person.

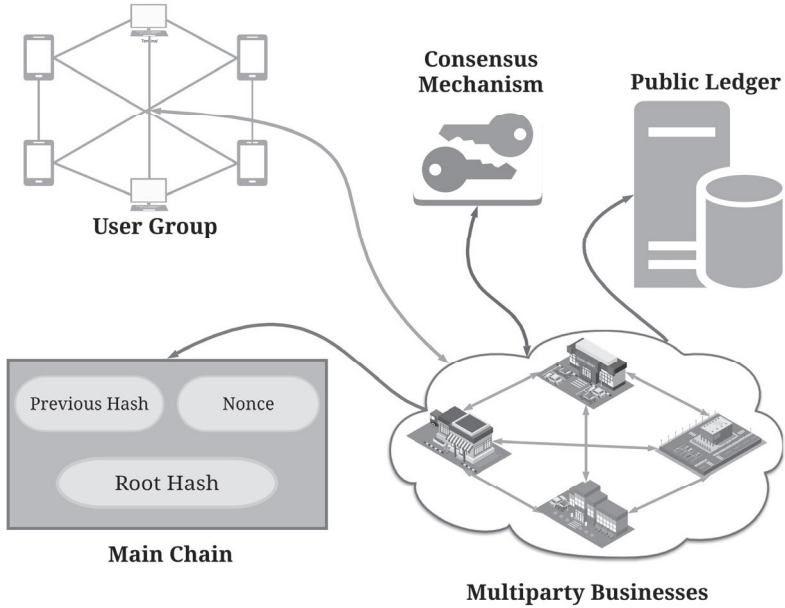


Figure 6: Implementing Blockchain for Industry 4.0 Applications

6.1 Securing Decentralized Information Processing

The main advantage of blockchain technology is that it operates without the presence of a central administrator or data storage capability. We can also refer to this as an interconnected set of blocks where each block contains a list of transactions, a time stamp, and information on the previous and next blocks. This feature makes blockchain extremely strong, immutable, and secure. [1] [12]

6.2 Ensuring Data Integrity and Privacy

Blockchain technology can be extended for an organization, to include its partners, customers, and supply chains, offering more opportunities to perform collaboration outside of the company's ecosystem. The distributed ledger means that a single version of the document is used, and can ensure that the activity is visible to everyone. Equal access is enjoyed by each party, so that there is less chance of data being hidden or manipulated, as no single party has full control over the database. [14]

6.3 Multiparty Interaction through Integrated Infrastructure

Blockchain uses decentralized, distributed storage to store transactions. In essence, this is a database which is spread over several platforms or devices in the network, which can store either the whole database, or a part of it, using a peer-to-peer network. In effect, this feature enables the integration facility among the different business organizations, which includes its partners, customers, and supply chains. Through this network, a distributed, but integrated, infrastructure can merge all the business which takes place in a smart city.

6.4 Influencing the Outcome of the Economy

It is a crucial job for a manufacturer to ensure product quality within its supply chain. However, blockchain is facilitating trustworthy, transactional, information keeping, in the digital ledger. This immutable ledger ensures product quality by checking the right materials are blended with the appropriate manufacturing process. This is the development of the 'outcome economy' which is set to change the plans of action for future business opportunities.

6.5 Rethinking Blockchain Integration

Customization of products is dynamic in nature, and therefore, rethinking blockchain to improve the quality of products is required. Thus, the higher risk areas need to be the greatest concern, and necessary steps need to be applied to the technology to ensure better security. Businesses will be influenced by the change of technologies. As the technology is continually improved, business owners or leaders should adopt it. They should consider changes by finding out how their businesses will benefit by integrating these advanced technologies. [15]

7. Uses of Blockchain in Industry 4.0

Smart warehouse and assembling, smart product, and smart city, are the principle practices of Industry 4.0 which are utilizing blockchain. [13]

7.1 Smart Warehouse and Assembling

Warehouses are becoming dynamic, intelligent, and autonomous, with the implementation of the fourth industrial revolution. As multiparty

transactions involve the supply chain, data visibility becomes a problem, which then makes the occurrence of misrepresentation and false accounting almost certain. Manufacturers can benefit from outside assistance with blockchain, which takes out the necessity of a central processing system to deal with all exchanges, and reduces the risk of alteration or other fake practices. Smart contracts and decentralized autonomous associations can make organizations progressively self-governing and increasingly wise, empowering machines to undertake quicker action by taking them away from human authority. [23] [13]

7.2 Smart Product

Smart product involves real time learning, and adaptation of production methods. Integrated working and learning processes are required to improve the quality of a product. By using the IoT and Industry 4.0, stakeholders will become involved with the development of smart product. A secured trustworthy data management system for smart product can be ensured with the use of the consensus mechanism of blockchain. Furthermore, smart contract ensures the authentication process which is required to access or change the data in the ledger. [13]

7.3 Smart city

Smart city incorporates six factors in its advancement approach: smart portability, smart economy, smart condition, smart individuals, smart living, and smart administration. By consolidating the internet, a remote broadband system, and sensor systems, the IoT will speed up the improvement of another age of IT and learning-based economy. Blockchain builds trust in businesses with its immutable digital ledger and smart contract features. However, this feature improves the personal satisfaction of the citizens and makes the city sustainable. [13] [14]

8. Constraints of Industry 4.0

Earlier, we defined the two major issues of Industry 4.0 which are most allied to blockchain technology, which are security and trust. But in general, there are some other key constraints that need to be addressed to achieve the fully-fledged value of the Industry 4.0 revolution. Technological advancement because of the presence of Industry 4.0 seems a blessing for the industrial revolution, through the use of IT, the IoT, blockchain, cloud computing, big data, robots, etc. This also raises some

challenges while taking advantage of the use of the above technologies in reality, and it requires dominant and combined efforts by the body that implements and governs this industrial revolution. Otherwise, it will not take long to notice the adverse effect of issues like security in the cyber world, protection of information, loss of integrity while exchanging information, interruption of automation while necessary, and the people in an organization keeping pace with the stream while implementing new standards in the work force.

Interlaced effort among the different parties to achieve the benefit of Industry 4.0 also raises some security concerns that need to be mitigated to make the participants comfortable. Each participating party has the right to handle their important information in such a way that it won't be misused or distorted by any chance. In this cyber physical world, the smart device plays an important role in every production system, and cloud computing does the job of building up connections among smart devices which, in the long run, opens the door for intruders to manipulate the confidential information they discover. This manipulation of confidential information incurs the loss of integrity that might disappoint the stakeholders and prevent them from being involved in the pace of Industry 4.0. In the context of automation and autonomous communication amongst different entities in the cyber physical world, the governing rules, followed by the process, must be free from any kind of misleading action by outsiders, and produced or consumed data must be in safe hands. [20] This, correspondingly, requires the protection of one's intellectual property, ensuring interoperability on different platforms for performing autonomous communication, and preservation of privacy in handling confidential information. This safeguarding can be achieved through the combined effort of all the participating entities involved in the industrial revolution towards Industry 4.0. [22]

In the pace of industrial revolution, Industry 4.0 becomes a blessing for people involved in production and development, through the revealing of technological advancements, such as blockchain, big data, the IoT, etc. But the implementation of this technology requires a unified process to be followed, so that all the participating parties following the Industry 4.0 revolution can benefit in the same way, irrespective of geographic location. This will call for a public standard to define the procedure that can be adapted while the different technological advancement of Industry 4.0 is realized by the concerned parties. [8] As when any recent technology, such as blockchain, is implemented, it needs to be done by

following the standard, so that the features of the technology can be realized by the different communities in a unified way, to reproduce the result successfully and easily. Otherwise, in a heterogenous environment, it will be challenged by interoperability and smoothness issues. [22]

Automation in production and development, which is the central concept of the smart factory [22], is one of the key blessings in the revolution towards Industry 4.0. Automation, in this context, makes the development and production system faster and firmer. But automation doesn't just mean using the capability of machines in the context of development and production systems. Rather, if the human creativity and capability of machines can be applied concurrently this will provide much better results, instead of rendering human labor obsolete. [26] Thus, no work force crisis will be created by not having human involvement in the organization. Companies can think about the contribution of human labor which will be mixed with machine automation in their strategic work plans and further decision-making processes. The decision-making process will be more bulletproof and controlled by utilizing the capability of human and machines together. So, machine automation in development and production will not replace human creativity, and humans have no fear of losing their position to machines. Furthermore, in the advancement of technology, new scope will be created that might require special expertise. So the human resources of the organization have to keep pace with the new requirements and challenges to follow the stream. On the other hand, organizations have the responsibility to train their human resource to prepare for new technological needs and future demands. [19] It is very obvious that in the pace of industrial revolution, new opportunities in the workforce will be created as time passes. Then new becomes old, and in the worst case, it might become obsolete. So, it requires combined efforts by all the participating entities to introduce development programs for their human resources to face the challenges of new technological trends. In this way, professionals will have the ability to deal with new technology, and the tools that will be required for increasing the workforce capability. [22]

In order to gain the advantages of industrial revolution towards Industry 4.0 all the enterprises have to participate at this pace. Not only should the large organizations be prepared for this revolution, but small and medium companies will also grab these blessings by making themselves ready for Industry 4.0. This isn't possible for them to achieve alone. This has to be achieved by integration with the global market. [4] Only then will

companies have the option to monitor the market situation, and see how the large companies take necessary action to take the advantage of technological development. To improve their offered services and products, small companies must have access to the right data and information from leading-edge organizations. This has to be done as it is a matter of small companies' survival in the competitive course of time. In the long run, it will help them to take advantage of cutting-edge technology, achieve enriched delivery of products and services, manufacture in an efficient way, reduce overall production costs, and establish themselves as strong competitors in the market. [22] Small and medium-sized companies should have the ability to adapt the latest technology and trends which are followed by the large and successful companies. To this end, all existing companies will have the capability of working together to achieve a common goal towards industrial revolution. In this way, the risk of not being compatible might be reduced, while the common interest among small and large companies can be synched. [21] Governments can be key players to facilitate all the necessary steps that the company needs to follow, to ensure acceleration in their workforce.

Execution is not the only way to gain the fully-fledged advantages of advanced technology, revealed in Industry 4.0. Rather, conducting research into specific needs also helps. And conducting research requires a collaborative approach by players who are active and aware in this stream of industrial revolution toward Industry 4.0.[5] The key players have to reach an agreement to work for a common objective, and the focus should be the same to conquer the mutual benefit.[6] Collaboration will help the participating entities to share and exchange the information crucial for their business need, to meet their demand, and implement their strategic business plans, utilizing the latest technology. In this regard, cloud service and blockchain technology perform an important role. Cloud service provides the opportunity of storing and distribution of information to the stakeholders on a real time basis that will, in the long run, enable them to achieve a better production system, improved business planning, and efficient management of human resources through better training. Blockchain will allow the key players of this industrial revolution to achieve distributed trust, and ensure proper security measures among them, which are key for the collaborative way of doing things. [9] [22]

9. Comparative Study of Systems Implemented With, and Without Blockchain

Blockchain is one of the key blessings of the industrial revolution towards Industry 4.0 that provides significant improvement in ensuring trust, in a collaborative approach to deliver service. This has been possible through the introduction of distribution, and transparency in trust in real time, that evaporates the need for an intermediary authority for verification and validation. [10] This further lowers the cost requirement for hiring an intermediary body, so obviously, this will increase the profit margin of the company implementing blockchain. The necessity of blockchain is revealed in the industry because of the lack of trust in the traditional way of verifying and validating transactions. This lack, in the long run, affects the financial gain of the company, as it requires spending extra money to verify and validate a transaction. This sometimes creates barriers in developing healthy relationships amongst the participating entities. Besides, fraud cases might generate a huge financial loss for the organization if the verification authority is compromised in any way. So, companies have to accept this kind of uncertainty in their trading as many parties are involved in the process, such as manufacturers, suppliers, and distributors. Transparency in trust is one of the key issues among parties to jeopardize the uncertainty condition. In order to eliminate this uncertainty, an auditing or intermediary body, which can convince all participating parties about the validation of the transaction being occurred, is needed. This auditing is, for sure, not free of cost. Companies have to spend much money to include the appropriate authority to run a business deal smoothly and in a trustworthy way. [10] A company has to make this flank investment for the sake of ensuring trust in a transparent way. This drawback of traditional transaction systems raises the need for mechanisms that eliminate the need for intermediary authority, and ensure transparency in trust in transaction processes which happen within multiparty relationships. The distributed trust feature also builds strong relationships in conducting business among parties. Fraud cases are eliminated, as there is no question of compromising the intermediary authority, which is totally absent in blockchain technology. Besides this, there is no delay in ensuring trust is tolerated in blockchain technology, as real time transparency is provided in a distributed manner. [10] As a result, the true financial status of a company can be easily known to other players, and this gives all the participating entities confidence to run their business with each other without being worried about the risk of any occurrence of fraud. This, at the end, reduces the surveillance cost. [10]

So, when a company takes advantage of blockchain technology, it eliminates the costs associated with verification and validation by the auditing authority. This provides a strong podium on which to conduct business, on any scale, among players realizing blockchain technology.

10. The Future Business Model

With the advancement of blockchain, the change towards Industry 4.0 has produced an abundance of new innovation. This engaging development ensures that the advanced physical structures making up keen processing plants are empowered to perform secured and autonomous requests. As the faults of the supply chain process can be traceable before production, it will cut down energy consumption. Blockchain's potential empowers us to adjust with others in increasingly effective, adaptable, and advanced plans of action which are dependent on safety and faith, considering all the factors. This anticipates blockchain to be a faithful partner in improvements related to Industry 4.0. [23] [16]

The processes, from the production line to the end user, offer extremely valuable data that may demonstrate importance to all concerned. End users know about this; hence the developing enthusiasm for discovering the accurate recognition of the items they purchase, and uncovering data on the commitment of every individual from the esteem chain. In any industrial condition, also, it is vital for organizations to monitor how parts are working or what temperatures they have been presented with. Blockchain can be utilized in both these situations, offering detection of any organization's exercises and activities; this is specifically noteworthy to the end client. Organizations can, likewise, enhance start-to-finish storage networks to the executives, including increasingly business-orientated rationales, and taking advantage of information received from IoT sensors, ensuring the reliability of this information, and limiting misrepresentation. [16]

Blockchain could make its mark. For instance, an integrated vehicle parking system will utilize the parking centers within a location (city) and information is going to be stored in the ledger. As per immutability of the ledger, the business information will be in sealed form, and a smart contract will help to authenticate any user. [2] [1]

To put it plainly, blockchain development in Industry 4.0 fills in as an intelligent stage, offering us an entire host of chances. Blockchain guarantees a more elevated amount of computerization, and removing

conflicts among parties. In this way, it is slicing expenses and accelerating information, with the net consequence of more prominent framework adaptability. It may be designed in various approaches to suit distinctive esteem chain forms, contributing immense advantages for everyone concerned, i.e., a client appreciating a high level of self-sufficiency and industry can turn out to be progressively effective by striking the correct harmony among free market activities. In this manner, machines will have the capacity to consult among themselves, making installments, or requesting supplies of their own. Finally, it welcomes things to come to the business.

11. Summary

- **Industry 4.0** helps to create the opportunity for building new technologies, to serve the mounting growth of smart systems, and to fulfill the demands of digitized society. The IoT, cloud computing, and big data, are directly associated with Industry 4.0 for the development of smart systems. The uses of the IoT, and the cyber-physical system, creates a real-time interactive system, and is the scope for making a decentralization process.

- Current trends and technologies are included in the fourth industrial revolution, and are also generating new scope for creating a smart system in a better way. **Smart warehousing**, **3D printing,** and **autonomous learning robots,** make the system more reliable, fast, and smart.

- The integrated service produced by Industry 4.0 is addressing some emerging issues. **Data security** and **privacy** are the main concerns in implementing Industry 4.0 based applications.

- **Blockchain** technology makes the integrated systems more reliable and trustworthy. Hence, the user does not need to rely on any third party trusted authority to make transactions. The security challenges related to Industry 4.0 have been minimized through blockchain implementation.

- The key features of blockchain are smart contract, cryptographic consensus mechanism, and distributed ledger. Blockchain can provide trusted distributed authentication and authorization through smart contact. And cryptographic mechanisms deal with the needs of data validation in the ledger.

- Smart city, smart product, smart warehouse, and assembling, are the applications of the fourth industrial revolution. The integration of blockchain reduces the safety issue, and additionally contributes to improving the framework's scalability.

- Blockchain plays a vital role in integrated systems, and can validate new transactions, preserve transaction transparency, and secure data transmission without the use of a trusted third party.

References

[1] S. Ahmed, S. M, M. S. Rahman, and M. S. Rahaman. A blockchainbased architecture for integrated smart parking systems. In *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, 2019.

[2] M. A. Al Maruf, S. Ahmed, M. T. Ahmed, A. Roy, and Z. F. Nitu. A proposed model of integrated smart parking solution for a city. In *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, pages 340–345. IEEE, 2019.

[3] A. Bahga and V. K. Madisetti. Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications*, 9(10):533, 2016.

[4] COMM/JRC/J2/. Smart specialisation platform, 2017. URL http: //s3platform.jrc.ec.europa.eu/sme-integration-to-industry.

[5] H. Kagermann, J. Helbig, A. Hellinger, and W. Wahlster. *Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry; final report of the Industrie 4.0 Working Group*. Forschungsunion, 2013.

[6] T. Kaihara, Y. Katsumura, Y. Suginishi, and B. Kadar. Simulation model study for manufacturing effectiveness evaluation in crowdsourced manufacturing. *CIRP Annals*, 66(1):445–448, 2017.

[7] S. S. Kamble, A. Gunasekaran, and S. A. Gawankar. Sustainable industry 4.0 framework: A systematic literature review identifying the current trends and future perspectives. *Process Safety and Environmental Protection*, 117:408–425, 2018.

[8] A. Khan and K. Turowski. A survey of current challenges in manufacturing industry and preparation for industry 4.0. In *Proceedings of the First International Scientific Conference "Intelligent Information Technologies for Industry"(IITI'16)*, pages 15–26. Springer, 2016.

[9] A. Khan and K. Turowski. A perspective on industry 4.0: From challenges to opportunities in production systems. In *IoTBD*, pages 441–448, 2016.

[10] T. Ko, J. Lee, and D. Ryu. Blockchain technology and manufacturing industry: Real-time transparency and cost savings. *Sustainability*, 10 (11):4274, 2018.

[11] Y. Liao, F. Deschamps, E. d. F. R. Loures, and L. F. P. Ramos. Past, present and future of industry 4.0-a systematic literature review and research agenda proposal. *International journal of production research*, 55(12):3609–3629, 2017.

[12] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos. Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *Journal of Network and Computer Applications*, 116:42–52, 2018.

[13] Y. Lu. Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration*, 6:1–10, 2017.

[14] M. Marques, C. Agostinho, G. Zacharewicz, and R. Jardim-Gonc¸alves. Decentralized decision support for intelligent manufacturing in industry 4.0. *Journal of Ambient Intelligence and Smart Environments*, 9(3):299–313, 2017.

[15] M. Menting.Is blockchain a viable technology for industry 4.0?, Aug 2018. URL https://www.manufacturing.net/article/2018/06/blockchain-viable-technology-industry-40.

[16] E. P. Pascal. Blockchain drives industry 4.0: the future business model, May 2018. URL https://www.gmv.com/blog_gmv/language/en/blockchain-drives-industry-4-0-the-future-business-model/.

[17] A. Rossow. Bringing blockchain into industry 4.0, October 2018. URL https://www.forbes.com/sites/andrewrossow/2018/04/11/bringing-blockchain-into-industry-4-0/#d53d3f96dc7d.

[18] H. Rudman. Blockchain: the backbone for industry 4.0, May 2018. URL https://www.wallet.services/blog/2018/5/28/blockchain-the-backbone-for-industry.

[19] M. Ru¨ßmann, M. Lorenz, P. Gerbert, M. Waldner, J. Justus, P. Engel, and M. Harnisch. Industry 4.0: The future of productivity and growth in manufacturing industries. *Boston Consulting Group*, 9(1): 54–89, 2015.

[20] B. P. Santos, F. Charrua-Santos, and T. Lima. Industry 4.0: An overwiew. In *Proceedings of the World Congress on Engineering*, volume 2, 2018.

[21] R. Schmidt, M. Mo¨hring, R.-C. H¨arting, C. Reichstein, P. Neumaier, and P. Jozinovi´c. Industry 4.0-potentials for creating smart products: empirical research results. In *International Conference on Business Information Systems*, pages 16–27. Springer, 2015.

[22] J. Smit, S. Kreutzer, C. Moeller, and M. Carlberg. Policy department a: Economic and scientific policy-industry 4.0. *European Parliament*, 2016.

[23] W. Viriyasitavat, L. Da Xu, Z. Bi, and A. Sapsomboon. Blockchainbased business process management (bpm) framework for service composition in industry 4.0. *Journal of Intelligent Manufacturing*, pages 1–12, 2018.

[24] D. Vuksanovi´c, J. Ugarak, and D. Kor˘cok. Industry 4.0: the future concepts and new visions of factory of the future development. *Proceedings of the International Scientific Conference - Sinteza 2016*, 2016. doi: 10.15308/sinteza-2016-293-298.

[25] L. D. Xu, E. L. Xu, and L. Li. Industry 4.0: state of the art and future trends. *International Journal of Production Research*, 56(8): 2941–2962, 2018.

[26] P. Zheng, Z. Sang, R. Y. Zhong, Y. Liu, C. Liu, K. Mubarok, S. Yu, X. Xu, et al. Smart manufacturing systems for industry 4.0: Conceptual framework, scenarios, and future perspectives. *Frontiers of Mechanical Engineering*, 13(2):137–150, 2018.

Authors Biography

Sabbir Ahmed earned his B.Sc. in Computer Science in 2012 and M.Sc in Computer Science with Software Engineering Major in 2015 from American International University–Bangladesh (AIUB) located at Dhaka, Bangladesh. Currently he is working as an Assistant Professor in the Department of Computer Science in the same university. His research work focuses on the cyber security but not limited to that field. At present, his research plan and study concentrating on big data analytics for the distributed system.

Razib Hayat Khan currently works as an Assistant Professor at Department of Computer Science, American International University–Bangladesh (AIUB) Dhaka, Bangladesh. Prior joining AIUB, he worked as a Software Developer at Intelliview and PatientSky, Oslo, Norway. He

finished his PhD from Norwegian University of Science and Technology (NTNU) at Trondheim, Norway in Software Engineering and completed his post-graduation form The Royal Institute of Technology (KTH) at Stockholm, Sweden in Information and Communication Systems Security (ICSS). He worked as a visiting researcher at Duke University, North Carolina, USA, consultant at Ericsson, Lulea, Sweden and project member at University of Twente, Twente, Netherlands. He published more than 30 publications in International peer reviewed journals and conferences. He has given numerous talks in international conferences. He served as a Technical Program Committee member and reviewer in several international conferences and journals.

CHAPTER FOUR

BLOCKCHAIN AND FOG COMPUTING: FOG-BLOCKCHAIN CONCEPT, OPPORTUNITIES, AND CHALLENGES

ADAM A. ALLI[1], MUGIGAYI FAHADI[2] AND ATEBENI CHEROTWO[2]

[1]Islamic University in Uganda, Uganda
[2]Islamic University of Technology, Bangladesh

Abstract

Blockchain, and the internet of things (IoT) are interesting technologies evolving to maturity over a couple of years. Business models are shifting from the traditional set-up, with high IT infrastructural and maintenance costs, to purchasing cloud computing packages from tech giants, like Google, at cheap prices, based on the pay-as-you-go model. Nevertheless, cloud computing has its drawbacks, like unreliable latency, lack of location support, etc. To mitigate these drawbacks, fog computing extends the services of the cloud closer to the user. However, the fog also has its limitations, such as the transparency of transactions, data security, and privacy. Blockchain is an eventual solution to alleviate these limitations. Powerful components of blockchain, such as cryptography, consensus mechanism, shared ledger, and time stamping, provide transparent, immutable, traceable, and decentralized business information models that are different from the traditional ones. This has been demonstrated by its application in crypto-currency. The success of blockchain technology in the financial sector opens up new horizons to technological exploration. In this chapter, we discuss the blockchain and fog computing paradigm, and elicit opportunities that the two technologies, if combined, can bring to the internet of things' ecosystem-enabling environment.

Keywords: Big data, blockchain technology, consensus mechanism, crowdsourcing, cryptography, device to device communication, dew computing, fog computing, the internet of things, shared ledger.

1. Introduction

The internet of things, smart things, the availability of vast information generated from a variety of application such as social media platforms, big data, and crowdsourcing, have driven the information era in a new direction which has certainly changed the way man interacts with the environment. The mobile internet outburst has potentially enabled remote areas to share information with each other, thus making the world a connected global village. [1] The use of IoT devices, especially the smartphone, has led to a paradigm shift in the ways people connect with families, and colleagues at work, through Facebook, twitter, WhatsApp, Skype, etc. The ease of use of new technologies, and their speed and reach, have enabled people to create content, share data, and network at prodigious rates. [2] The economy has become globalized, and strategic activities can work as units on a planetary scale. [3] Security agencies can share crucial data to combat terrorism and crime. Farmers use modern mechanization embedded with the internet of things (IoT) devices to monitor farm assets, like soil quality and farm inputs, required to achieve optimum yields. Also, farmers use animal and disease trackers to professionally manage their farms. In addition, they use the internet to find a market for their produce. [3] Schools have benefitted in the same way, by creating content through crowdsourcing, big data, learning analytics, etc., and using the same data to tailor academic content in line with the industry. [4] Again, institutions of higher education are using machine learning on collected data (big data) to detect authentic documents. However, today's infrastructure is highly centralized, with data stored in centralized repositories, i.e. the cloud, and organizational data centers, which are owned and controlled by some central authorities like government, and multinational corporations (Google, Microsoft, Amazon, etc.). This gives rise to a number of concerns in relation to security, privacy, trust, and data control. [5] For that reason, there is a need to have an architecture that can enable peer-to-peer communication, and provide information security, integrity, and privacy. This same architecture should decentralize data storage, computing, and processing resources. Blockchain technology and fog computing, coupled together, can afford to solve the aforementioned traits.

The fog is viewed as one of the drivers, not only for the internet of things, but also as the primary enabler for 5G, embedded artificial intelligence (AI), and advanced distributed systems. [6] Fog computing is a paradigm intended to moderate the challenges of traditional cloud-based IoT systems. [7] The challenges of the traditional cloud include new use cases which require very low latency, real-time applications that need reduced communication cost at low risk, and applications that are security and privacy-sensitive. The fog supports real-time analytics, and mobility of IoT devices without loss of service and connectivity. The fog also takes care of network unavailability situations, especially in rural areas, where internet connectivity may not be as fast and stable, compared with urban areas. For that reason, many applications that could help users in those rural places are not implemented to the required scale. [8] Therefore, for applications that have dynamic features and produce huge amounts of data frequently, fog computing becomes an ideal solution.

The fog computing paradigm has its related drawbacks. Among them is the security of massive data, scalability due to large numbers of things that desire connectivity, and physical security of the fog device due to proximity to the edge of the network. The aforementioned drawbacks do not only raise connectivity concerns, but come with aggravated trust concerns among connected devices. Concerns related to data aggregation, data integrity, and authenticity of users, all form the basis on which blockchain technology may be embraced in the fog environment. [9]

Looking forward, the scope of blockchain technology started with the success achieved in crypto-currency as a distributed leger technology. Today, it is hoped that blockchain technology will be embraced in many places, which include fog computing. Blockchain technology is able to guarantee a safe transaction in a highly untrusted environment. Moreover, blockchain can accelerate transaction among peer-to-peer devices. For example, in fog-blockchain-supported infrastructure, a fog node, IoT device, or another edge device, may be equipped with smart contracts, which outline the behavior of each device. Based on the behavior, devices can perform secure transactions without any third party (human) to ‘certify’ their transactions. Further, blockchain technology ensures trustable architecture, increases adaptability to massive network devices, and eliminates single-point-of-failure in a precise manner. Blockchain in a fog environment will decentralize authority, enabling a completely trustworthy digital infrastructure. [10]–[12]

The need for a fully decentralized, trustworthy, fog infrastructure cannot be underestimated, given the current trends in the IoT world. Cisco [13] predicted the internet base to be 50 billion devices by 2020. Adoption of use cases, such as connected cars, connected hospitals, crowdsourcing applications, and smart cities is on the rise. Applications cutting across use cases, such as connected planes, are projected to produce five terabytes (TB) of data per day. Smart hospitals are projected to produce three TB of data per day. Connected things in factories and industries are projected to produce three petabytes (PB) of data per day. Intel has predicted that self-driving autonomous cars will produce four TB, per car, per day. Interestingly, projections have it that an individual person will generate and use up to 1.5 gigabytes (GB) of data per day in the near future. [14] All the above are signs that call upon a shift of operations, and functions, at both the cloud and edge technologies. Blockchain technologies will shift how the fog-cloud of things operates, tremendously. It will bring to life the 5G dream of almost zero latency and secure transactions. [15]

This chapter, therefore, will address the advent of the fog-cloud-of-things and blockchain technologies. This is done by examining its applications within the building blocks of fog computing that appeal to the users of blockchain technologies.

1.1 Chapter Roadmap

In this chapter, we present the fog-blockchain framework, opportunities, and challenges. Blockchain technologies provide enriched opportunities to advance the distributed internet, keeping in mind trust, security, and efficiency, in transactions at all levels. In section 1.2, we introduced the basic concept underlying the internet of things (IoT), fog computing, and blockchain. We present the fog-blockchain and its application paradigm, opportunities, and the challenges of adopting blockchain technologies, in sections 1.3, and 1.4, respectively. The conclusion and recommendations are presented in section 1.5.

2. Definition of Concepts

The future requires that storage, computing, and analytics, be distributed along the network hierarchy. This is paramount because new upcoming use cases, such as the smart city, smart grid, smart environment, etc., need speed, security, scalability, and operation at low cost. These factors will define new trends in computing and communication. Blockchain and the

fog are viewed as things which will bring flexibility to deploy at the edge, and seal the dream of 5G, known to be the next generation radio access network. This supports communication with ultra-low latency, provides massive machine-to-machine communication, enhances mobile broadband, and brings on board ultra-reliability. Moreover, it guarantees security, privacy, and trust. Other sources of inspiration for blockchain are found in the secure device on board, time-sensitive networking, and functional safety. Below, we give the concepts underlying the internet of things (IoT), fog computing, and blockchain technologies.

2.1 The internet of things

The internet of things (IoT) is a new formation, which is projecting information and communication technology (ICT) in a new direction. The formation is promising to bring connectivity to all things on the face of the earth. The concept of the 'internet of things' is not a toolkit of science fiction any more, but a crucial component of regular lives. [16][17] The IoT is a technological revolution that represents the prospect of computing and communications. Its development yields dynamic technical innovation in science, technology, and engineering. [18]

The ability to digitally label and track things has allowed companies to become more efficient, speed up processes, reduce errors, and increase security in organizational processes. Organizations are able to incorporate complex and flexible systems in the organizational ecosystems through the use of the IoT. [16] [18] [19]

The IoT is continuously evolving, and provides infinite opportunities for users, developers, and enterprises. The concept of enabling interaction among things is leading-edge technology. With the IoT, data can be obtained from all kind of objects, and sent for processing to various virtual platforms existing on the internet infrastructure. This results in: i) massive amounts of data to be gathered from things in a short time; ii) the need for high processing power; iii) secure processes distributed along the internet infrastructure to support massively ubiquitous devices.

The vision of the IoT is hinged on creating an environment in which things are able to communicate with each other and exchange data through intelligent means. Significant decisions have been taken by IoT players like Cisco, Google, Apple, Samsung, Nokia, Microsoft, etc., and telecoms operators have positioned themselves in the design and development of

IoT hardware and software solutions, standards, architectures, and protocols, for current and visional IoT devices.

The IoT landscape consists of D2D (device-to-device communication), and M2M which promotes communication between devices, such as smartwatches and phones. They can be useful in controlling and monitoring, and services access provision, such as printing, security access keys, shopping, etc. They provide fast communication to a theoretical range of 200m. In the future, as the technologies mature, uses of D2D are likely to increase beyond sharing and controlling data.

Machine-to-machine and the IoT are focuses for core business, which result in the rapid growth of connected objects within their network. [19] As one of the critical technical enablers for 5G networks, device -to-device (D2D) communication provides an efficient alternative to cope with the requirements of massive machine type communication (mMTC) services. [20] [21]

The motivation for exploiting device-to-device D2D communication is to enable data exchange for ultra-reliability and low latency. [22] [21] D2D communication has been standardized to enable discovery and communication between two devices. The Third Generation Partnership Project (3GPP) specifies the basic D2D communication motivated by public safety communications, in Release 12. This standard goes on to incorporate use cases beyond proximity services (prose). Further improvements in standards have been made to incorporate the service requirement of 5G, including the support of connections without network devices in the middle, as seen in 3GPP Release 15, and connections supported through relay equipment (indirect communication). [23] [24] Preservation of energy has been explored, so as to adapt and evolve legacy networks as one of the core technologies around D2D. [25]

The IoT is increasingly pervading our lives, where the last connected things are not only mobile devices such as smartphones and tablets, but also smart TVs, cars, refrigerators, smart lights, and bulbs. IoT devices are being connected at a prevailing pace. Experts forecast that 25 billion devices will be connected by 2020. Devices without the internet will have to upgrade to some form of connectivity, using frameworks such as Arduino, NET Gadgeteer, Lego Mindstorms, etc. [16]-[26]

The need to combine secure interactions between several devices, such as in machine-to-machine (M2M) communications, has yielded noticeable

standardization efforts. With the number of IoT devices increasing, the communication of devices becomes more complex, leading to less human contribution. IoT devices are no longer just communicating explicitly with each other, like traditional computers or smartphones. They can be controlled indirectly by other multiple devices, actions, or environmental conditions. Using services like IFTTT (if this, then that), useful traits of learning, generalization, optimization, and adaptation, are possible. Scenarios that belong to IFTTT are popular in various IoT applications. For example, if the thermometer detects that the indoor temperature has raised above the threshold, the smart device plug detects the air conditioner is in the 'off' state, and the windows will automatically open. Similar examples are more common in industrial and agricultural devices (e.g., automatically adding more water into smelters according to temperature and humidity, or automatically turning on sprinklers, if moisture content is low). [27]

As we prepare to embrace the ground-breaking impact of the IoT in our lives, the convergence of IoT devices with machine learning, artificial intelligence, fog computing, cloud computing, and blockchain technologies must be explored. This will enable companies to move from IoT initiatives that merely produce incremental gains, to those that create entirely new business models. [28]

2.2 Fog Computing

Nowadays, the number of IoT devices around the world is hitting 15 billion. These devices are not only numerous, but required to perform computationally intensive, and delay-sensitive, applications. These applications range from artificial intelligence, virtual reality, crowdsourcing, and distributed data analytics. In many of the aforementioned suites of applications, the computational capabilities of IoT devices do not prosper, due to low processing power, memory, cache, response time, latency, etc. This is partly because of the small form factor of the IoT devices. The requirements of size and weight do not allow IoT devices to be equipped with more powerful processing power, large storage devices, or heavy hardware that are required to run complex applications.

To permit progress in improving the computational capabilities of the IoT, computing paradigms, such as transparency computing, edge computing, and fog computing, have been positioned to redeem the drawbacks caused by large numbers, and small form factors of IoT devices. In all these paradigms, efforts to employ resource-rich devices at the edge, e.g., small-

scale servers, routers, switches, desktops, laptops, and other computing devices, to assist in handling computationally-intense and delay-sensitive applications, have been proposed. The fog, among other edge paradigms, is motivated to bridge computational processing, storage and latency problems in a cloud computing environment. Computational offloading and real-time analytics have emerged as applications which highly promote the use of fog computing. Computational offloading is a process that enables constrained low-end IoT devices to transfer computationally expensive tasks to either the cloud or edge platforms, which are resource rich. Whereas, real-time analytics involves getting insight from data as soon as the data becomes available. Up until recently, the cloud has been the better choice for offloading and analytics. The cloud exhibits numerous advantages, including cutting across abundant resources, secure computing, and fast processing.

Naturally, the cloud provides cheap initial setup, reducing companies' worry about the initial cost of establishing an information technology infrastructure which can take care of storage, analytics, and other data processing. It allows users to use the pay-as-you-go model to leverage the advantages of cloud computing, storage, and other services. Secondly, the cloud provides a flexible, abundant, amount of resources, such that users often need not worry about updating their hardware and software resources. Third, the cloud provides a high quality of control, in that all documents are stored in one location, in similar format. Every employee can access the same information, thereby avoiding inconsistencies in data, or human error, and it provides clear records of revisions and updates. Lastly, the cloud provides infinite computing, storage, and processing capabilities, that a single, or individual user cannot afford.

Though the cloud gives all the advantages mentioned above, it falls short in applications which have critical latency requirement, for example in intelligent transport systems, which have a latency requirement of fewer than 50 microseconds within a communication range of 500 meters, to ensure high reliability. Such applications require fewer network hops, lower focused loads, and lower transit time latency. Secondly, applications which require location awareness while remaining data rich, for example in vehicular networks, need the node to move from one place to another, while maintaining the ability to cache and process a correct piece of information. This is not limited only to vehicular networks; it also applies to portable human devices which are not stationary. These kinds of use cases require data located at an optimal depth from the source, so as to perform better. Thirdly, there are applications that use data that is location

bound and requires high security and privacy, i.e. some data may be required to remain within certain geographical boundaries, so as to preserve integrity, confidentiality, and authenticity. Examples of such applications include government applications, health applications, etc. Such use cases require localized intelligence which is often not provided by the cloud. Other cases which find the cloud less suitable are those in which bandwidth is constrained. For instance, consider a connected city application, with all the data transiting through a cellular network or satellite link, where a huge network operation cost is inevitable, and therefore localizing the processing of such data to reduce the core network load becomes a necessity.

Lastly, applications that require reliability and robustness find the cloud, not to be a suitable residence. In particular, those with a local emergency response requirement, or fast fail-over adjustments to a neighboring device, will not find the cloud useful. All the above-mentioned use cases, including those which perform analytics and storage at the right level, apparently require edge computing technology in the form of fog technology, which facilitates the operation of computing, storage, and networking services, between end devices and cloud computing data centers.

The concept of fog computing stretches from the outer edge where data is created, to, eventually, where it is stored. This storage location could be within the organizational data center or the cloud. It forms another layer of a distributed network environment, in between cloud computing and the internet of things (IoT), which provides a continuum to bridge the missing link for data that needs to be handled locally closer to the edge, or pushed to the cloud. Fog computing provides a horizontal system architecture that distributes resources and services of computing, storage, control, and networking, anywhere along the continuum from the cloud to the internet of things.

The fog extends computing, aggregation, and storage capacity, to applications that require: i) reduced latency and time-sensitivity; ii) high response time; and iii) security and privacy-sensitivity, and to those applications that are deployed in connectivity-constrained locations, especially in rural areas.

To conclude this section, we adopt the definition of the fog from Cisco, as “a decentralized computing infrastructure in which data, computing, storage, and applications, are distributed in the most logical, efficient place

between the data source and the cloud." Fog computing spreads out cloud services to the edge of the network, bringing the advantages of the cloud closer to where data is produced. The fog is required to improve efficiency, and decrease the amount of data transported to and from the cloud for processing, analysis, and storage. The fog computing infrastructure is suitable for new upcoming applications in smart cities, crowdsourcing, telemedicine, and real-time data analytics.

Other concepts related to fog computing include dew computing, cloudlets, mobile edge computing (MEC), and mobile cloud computing (MCC). Unlike fog computing, dew computing uses on-premise infrastructure that includes software and hardware independent of cloud services, and remains in collaboration with the cloud. In dew computing, devices can access a fraction of the web, such as its storage, databases, software, and software development kits, without internet connectivity. Projects in dew computing have a copy in the cloud infrastructure, such as in Dropbox, Github, Google play, and Google drive.

Cloudlets, multi-access edge, and mobile cloud computing are closely related to fog computing in terms of operation. They differ in terms of compatibility, the number of active users, flow characteristics, server density, coverage, and ownership. For example, the cloudlet is less compatible for use cases in smart grid and connected vehicles, while the MEC is less compatible in use cases in body area networks and healthcare, face recognition, smart grid, military, and hostile environments. In general, the term edge computing is used to comprise the fog and all other related concepts.

2.3 Blockchain Technology

Blockchain technology is basically a distributed database (ledger) that builds an immutable list of time stamped transaction records. [29] Each blockchain is encrypted and organized into smaller datasets, called blocks. Each created block contains information about a number of transactions in reference to the preceding block in the chain, and a mechanism to answer a complex mathematical puzzle. Once a block has been added to a chain, it cannot be deleted, and it is distributed to all clients in the peer-to-peer network. [30] Blockchain technology is powered by peer-to-peer networks, consensus-making, and cryptography. [29] Each block created has a hash (H) generated from the content of the transaction (C) and the hash value (h) of the preceding block in the chain. To generate the hash (H), if the content of the transaction C = 'Transfer $1000 to Fahadi', then

C is XORed with the hash value (h) of the preceding block using a given hash function h(c). The hash value plays two important roles that are to uniquely identify the block, and identify the order or position of the block in the chain.

Naturally, after creation, a full copy of the blockchain is stored on each node on the network which is achieved through periodic synchronization. Therefore, in the simplest sense, a block is a collection of all the recent transactions that have happened, and are verified by the miners, and have attained a 51% network-wide consensus. Blockchain has most successfully been applied in cryptocurrencies such as bitcoin, where transactions are straight between the owner and the receiver, broadcasted through peer-to-peer networks without any intermediate party, such as a bank, multinational cooperation, or government. Further, they achieve the same functionality and certainty as a centralized infrastructure, but the transactions are made publicly, and anonymously.

3 Fog Blockchain Environment

The fog computing ecosystem is a distributed computing one, which presents challenges ranging from how to protect network resources and transactions at the same pace of distributed security structure, to issues related to scalability, deployment, resilience, and availability. The fact that fog computing creates vast fog nodes, spread along a mesh structure, with almost equal responsibility and roles, creates a new challenge. Therefore, together with distributed computing, we need to have distributed security, privacy, and trust. This attracts even more attention if the infrastructure and layers of the fog stack are owned by different entities. The question of managing trust in a decentralized, distributed manner, among nodes that might not necessarily trust each other, has been visualized using blockchain technology. The blockchain technology enables the fog ecosystem to become fully decentralized, and gives the ability of true redundancy, in which discrete nodes are intelligently distributed along with the globe. This is true for all the configurations of the fog that use cases where different fog nodes need to work together, though they may not trust each other, and disconnected or autonomous systems.

In an event where fog technology is becoming an important part of the internet of things (IoT) and 5G applications, there is an increasing need to influence distributed ledger technology to create consensus for each transaction. Due to the different requirements (computing power, memory,

bus speed, etc.) needed for the consensus mechanism, some mechanisms may fail to meet applications in the fog ecosystem. For example, the proof of work' consensus requires heavy computation capacity to solve its puzzle, and therefore attracts less interest to be hosted on the IoT or fog nodes with considerably low computing power, whereas the 'proof of stake' consensus is capable of running on fog nodes of the same capability. As a result, efforts to incorporate blockchain into the building block of the OpenFog standard consortium, to realize interoperable and composable architecture, is underway.

Companies such as sonm (https://sonm.com/), hyperchain (https://www.hyperchain.cn/), and keychain (http://www.keychain.io/) have joined hands in developing blockchain solutions at the same time, contributing to OpenFog. In order to enable blockchain horizontal use cases in which distributed system providers can commoditize and sell fog computing resources, with the assurance of being paid for these services, standards must be embedded in OpenFog. Currently, the Open Fog Consortium is working on setting up the foundational requirements to enable distributed ledgers.

The blockchain technology enables the fog-cloud of things ecosystem to become fully decentralized. This gives true redundancy in which discrete nodes are intelligently distributed around the globe, in addition to facilitating the use of the resource on demand, in that some other services are obtained at a cost. Blockchain provides means through which payments for these services can be automated. Moreover, to resolve security issues, a mechanism in which users maintain their own keys is provided. Each node stores fragments of user data, hence achieving complete privacy, trust, and control. Lastly, quality of service and quality of experience can be achieved at significantly low cost, by first tracing resources, second, auditing the existing services, third, executing electronic services level agreements, and lastly, eliminating the middle man, so hire of services becomes cheaper.

3.1 The Fog Cloud of Things- Blockchain Fog Architecture

The fog emerges as a computing model that brings computing capabilities to the edge in a distributed manner. This allows for the services that could otherwise be provided by the cloud to be provided at the edge. In so doing, use cases that require very low latency, applications that are power hungry, those that require real-time analytics, and security- and privacy-sensitive applications can be served at the edge of the network. Moreover,

devices can gather locally, categorize, and analyze data, thereby increasing the speed of processing large amounts of data that could not otherwise be sent through the core of the network. Also, the secure deployment of fog nodes and cloud computing resources ensures that communication between the fog and the IoT is achieved with fewer constraints. IoT devices access computing resources anywhere, at any time, and low end-to-end delay is achieved with less increase in network traffic.

i) The IoT Devices: The IoT devices acquire, monitor, and measure data. In addition, they send and receive data to and from the fog and/or the cloud. The public infrastructure environments created by the IoT devices allow them to monitor and filter data for local consumption. IoT devices are characterized by low computational power, and constrained by battery life and form factor. They have considerably low memory and are powered by small battery cells. They are widely deployed, spreading across cyber-physical systems to smartphones. There, form factor enables them to be embedded in all types of device, including human beings, animals, vehicles, airplanes, fridges, cookers, factories, surveillance cameras, etc. IoT devices may be installed on a static object or a mobile object.

ii) Fog devices: Fog devices consist of high-performance distributed components. Fog devices report the results of processing to both cloud and IoT layers along the continuum. They may be mobile or static. Unlike IoT devices, fog nodes are more powerful, and can provide localized services when the need arises. They can provide considerably long-time storage of data, and perform data analytics at the transactional level. Moreover, they can support IoT devices by providing services such as computational offloading, distributed security, privacy, and trusted transaction. Similar to the work in Sharma, Chen, Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT" (2018) [10], the fog can be powered with analysis function, packet migration function and security function to take care of security, privacy, and trust functions of the network. At the fog layer, the system consists of a smart gateway fitted with interfaces whose function is to adapt the network to new technologies that are based on the IoT. Smart gateways can aggregate raw data from IoT devices, monitor traffic, and forward data. Each fog node may be equipped with a software-defined controller, whose purpose is to provide a programmable interface, intelligently distribute workload, and perform network management and other essential network functions. The fog can offload either its data, or processes, to the distributed cloud, in case it does have enough computational capacity to handle the task received. Extra cost, such as energy consumption, delay, and cost of usage, may be

accrued. A dynamic framework such as in [31] [32] [33] can be adopted herein.

iii) The cloud: The cloud consists of very powerful, start-of-the-art centralized infrastructure, which has an infinite capacity to realize secure and heavy computation. In this era of massive data production, most of the data produced by devices are ephemeral, and attract less value to be sent back and forth to the cloud. Secondly, the nature of the application at hand may need to be handled by a new cloud infrastructure. A distributed blockchain cloud opens up opportunities for expanding the use of existing cloud infrastructure, putting together data of users, producers and consumers. Given a list of service providers, users select a resource provider from the distributed blockchain cloud infrastructure and services, before the required service is provided. The services may include, but are not limited to, data processing, storage, platform, executions, data management, and server provisioning, etc. On receipt of the request, the service provider registers the transaction in a blockchain, and lastly, the providers will be paid and rewarded. [10] In this architecture, a reward system guarantees the quality of service and transparency of the system, and ensures that consensus as to who provides service, and how, is reached. A number of consensus mechanisms that are applicable in this situation are discussed herein.

3.2 The Application of Blockchain in the Building Blocks of Fog Architecture

The application of blockchain in the building blocks of fog architecture may not attract better use incentives for all types of fog transactions. Some applications may find the use of directed acyclic graphs or database better than the use of blockchain. Topographies that attract the use of blockchain include: i) applications that demand decentralization when no trusted centralized system exists; ii) applications that encourage peer-to-peer communication especially in intelligent swarm, and communication among nodes at the same level, as in fog architecture; iii) applications that require economic transactions to be performed without third parties, although in some situations it is still better to include a third party; iv) applications that need to keep a record of every transaction to maintain traceability, for auditing purposes and to perform analytics in future; and v) robust distributed systems that lack some element of trust and privacy.

3.3 Key Features of Blockchain Fog Architecture

- **Cryptography:** Public-key cryptography forms the most essential component of fog blockchain technology. It is used to legitimize transactions. It incorporates security, privacy, and block chaining features. Cryptography is used to ensure the integrity of the messages, and signing transactions, and may be used to create a wallet in situations where cash transactions are required. It uses digital signature algorithms (DSAs) to create a set of new private keys that correspond to public keys. The public keys are used in a hash function to create a public address that users can use in their transactions. The private key is always kept a secret, and is used to sign a digital transaction. Digital signatures are used to sign an electronic document.

  Digital signatures perform the same function as physical signatures on physical documents. They are used to make sure that any user performing a transaction is the owner of the private key. This action is similar to the owner of a bank account signing a check/bank slip to verify he is the owner of the account which he intends to withdraw from. Digital signatures form a critical part of every transaction that happens in fog-block architecture. They guarantee transactions are true and remove the possibility of fakeness. Digital signatures depend on two basic functions, i.e., signing and verifying. To sign, the user needs a message and the private key. This allows him to produce a unique signature. After the transaction has been signed by the owner, it is placed in a memory pool for processing by miners. The miners use the sender's public key to ensure that the digital signature is authentic. This action cuts off hackers, in that they cannot seek services without permission. If the ownership and digital signature check out, the transaction is included in the next block, and the transaction is approved. Otherwise, the transaction is rejected.

  If a user says Alice wants to perform a transaction with Bob, he or she must first agree to transact over a blockchain network. Alice will broadcast her intent to transact over the network. No one can prove the integrity of Alice, because anybody can masquerade as Alice and broadcast the intent. To verify the integrity and authenticity of the message, Alice will sign her transaction using her private key, resulting in an authentic, signed transaction

request, which she will broadcast. This transaction will be placed in the memory pool. The next phase is mining. When a miner (Fahadi) receives this transaction, he runs the message through the function (algorithm), using Alice's public key as the input. If the signatures tally, then the transaction is confirmed to be authentic. This allows him to verify if the transaction is indeed from Alice. If the verification is true, the block is placed in the chain. Then Bob can receive the transaction. [34]

- **Time stamps:** Tracking modifications on the blockchain requires that transactions be signed and time stamped. Stamping transactions are performed in a synchronized way using time stamping servers. Traditionally, time stamping relies on the trust put in the server, though this does not stop the signing of past transactions. Proposals to include a hash of the previous time stamp have been explored later. [37] This makes it difficult to insert forged transactions amidst records of transactions. Moreover, time stamping can be distributed, so as to avoid a single point of failure.

- **Shared ledgers:** The major intention of shared ledgers is to eliminate intermediaries, and create transparency in the system. [30] Shared ledgers are used to enforce digital trust and bring the entire network to a single view. The immutable digital ledgers, implemented in distributed fashion, enable the community of users to record transactions in a ledger publicly, so that no transaction can be changed once published. [35] [36] When a single person wants to transact, he broadcasts the transaction to the whole network, where everyone records the transaction. However, if one of the members is greedy and changes his ledger, this causes disputes and clashes in the group, which brings us to the next feature of blockchain, called consensus.

- **Consensus:** The consensus mechanism determines the conditions concerning the validations of the blocks to be added to the blockchain to be reached before concluding an agreement. This mechanism is implemented using a consensus algorithm. The most ideal consensus can be achieved through 'one man one vote', i.e., each miner is assigned equal weight when voting, and the party that receives the majority vote, wins. This situation can only be achieved in a controlled environment. In a blockchain environment where one user may have multiple identities, this would not work,

because users with many identities may end up controlling the blockchain. The event in which single individuals with multiple identities take charge of a blockchain in order to influence its operation, is referred to as a Sybil attack. In a decentralized environment like the blockchain, one user is selected amongst the users to add a block. This can be achieved through random selection. The problem associated with random selection is that it is prone to some forms of attack. In order to avert attacks, a node which performs a lot of work on the network is not likely to be interested in attacking it. Therefore, choosing such a node to add a block in a blockchain is often feasible, hence the concept of 'proof of work' (PoW). In PoW, miners are required to perform an expensive computation task which is theoretically impossible to perform, using an individual entity, until a solution is found. The process is hereafter known as mining. Once the solution is found, it becomes easy for other miners to verify that the solution is correct. This activity helps separate all the fraudulent transactions as computationally infeasible.

Proof of work (PoW) uses a 256-bit hash function called SHA 256, which takes in any kind of message (transaction), and produces a message digest. For example, a user is assigned a task to take all the transactions in the ledger, add a nonce at the end of each, and apply SHA 256 on it, such that the first 32 bits are all zeros. The probability for a user to guess the answer is one in a billion, since SHA 256 is a cryptographic hash function. The only way to find out is to guess and check, meaning users have to go through a billion guesses to come to the output. This task, in essence, becomes computation-heavy, but once the user finds the output, it becomes easy for other users to run the hash and compare the results. [35] The drawbacks of PoW are seen in heavy resource consumption and scalability, and the majority of mining is centralized to where energy is cheap. The drawbacks mentioned here make PoW less attractive for IoT blockchain use cases, given that IoT users are constrained in both processing capacity and energy. Other consensus algorithms are desirable for the IoT ecosystem. Below, we describe other consensus mechanisms that may be better than PoW in IoT environments, as follows;

Proof of service: in proof of service, it is assumed that a node that contributes to some action outside the blockchain, such as performance of computation, transfer of files, or providing data that

leads to the occurrence of token exchanges between members of a network, is less likely to get involved in attacking the network. This variation of consensus requires proof of contribution. Proof of service gives a careful consideration, so as to eliminate claiming illegitimate rewards.

Proof of stake: this is an alternative to proof of work. Instead of investing in expensive computer equipment in a race to mine blocks, a validator invests in the participation (e.g. currency) of the system. [10] [12] In proof of stake-based blockchain, it is assumed that users with more participation on the network are less likely to attack it. Consequently, miners have to prove occasionally that they have accomplished a certain level of participation on the network. It is noted that validators are used because no currency creation exists in proof of stake; instead all the currency already exists, and validators are paid strictly in transaction costs. This consensus is cheaper in energy consumption than a proof of work consensus. There are a number of variations of proof of state consensus mechanisms, which include delegated proof-of-stake (DPoS), in which selected nodes are delegated to create and validate blocks. In such a case, fewer nodes are chosen to do the work and transactions as proof-of-stake, in which all nodes that are involved in transactions contribute to the security of the network.

Proof of burn: this is a consensus method that requires miners to show proof of their commitment to mining by burning some cryptocurrency through an unsuspendable address. The idea behind PoB is that, instead of burning resources, it is better to spend currency. The user burns coins by sending them where they are irredeemable, thereby gaining a lifetime privilege to mine on the system, based on the random selection process. Depending on how proof of burn is implemented, miners may burn native currency, or that of the alternative chain, like bitcoin. [38] The more coins you burn, the better chances you have to mine the next block.

Proof-of-activity (PoA): consensus algorithms are proposed due to the main limitation of PoS systems based on stake age: proof is accumulated even when the node is not connected to the network. Thus, PoA schemes have been proposed to encourage both ownership and activity on the blockchain.

Proof of elapse time: this is similar to the proof of work, but consumes less energy. Instead of having participants solve cryptographic puzzles, each participant in the blockchain network waits for a random amount of time. After that, the first participant to finish waiting becomes the front-runner for the new block. The algorithm is based on two questions: i) did the winner actually choose a random wait time? and ii) did the winner complete waiting the specified time?

In general, the algorithm works as follows: i) a new user downloads a trusted code from the blockchain; ii) the trusted code creates a key pair; iii) participants send a request to join; iv) the participant obtains a signed timer object from the trusted code; v) the participant waits for the time specified by the timer object; and lastly, vi) the participant obtains a certificate and sends it to rest of the network. The origin of proof of elapsed time is Intel, and it relies on a special CPU instruction set called Intel software guard extensions (SGX). SGX allows applications to run trusted code in a protected environment. SGX ensures that the block gets produced in a random lottery fashion, but without required work. The entire approach is based on the guarantee with time provided. [38]

In a nutshell, there are a number of consensus algorithms created by different parties that may be applicable in the blockchain-fog ecosystem, as long as they are lenient in consumption of energy, and attract less processing power than the others.

4. Opportunities and Challenges in Adopting Blockchain Fog-Cloud-Things Paradigm

With the recent integration of smart-contracts in blockchain, devices can easily transact and settle obligations directly, without the need for human intervention. This blockchain feature can empower the fog to let devices directly transact with each other by paying for any service rendered by another fog device, for example, paying for any additional computing power or storage, and also the device being paid for any similar services rendered to other fog devices. [38]

With blockchain technology, it is possible to have a smart contract coded in a device (IoT devices and fog) to execute contracts without user intervention. Assume that an IoT seeks service from the fog, and that this

service requires a monetary transaction; the contracts between the IoT device and the fog infrastructure stipulate how much service the IoT is entitled to. Another way, is if a device has done some work which needs to be rewarded, the smart contract between the two will stipulate how much reward is required. The smart contract represents an ordinary contract, executed when triggered by conditions agreed by parties in the contract. Since smart contracts are designed and implemented within blockchain, they are immutable, self-executing, self-verifying, distributed, auto-enforcing, and trustworthy. Using smart contracts, direct payment between devices can be accomplished. This may find use in transportation and logistics, household, delivery services, warehouses, service industries, etc. Smart contracts open up a whole range of opportunities in fulfilling inter-device agreements, automatic and secure software updates, and service and resource bartering between devices, let alone machine-to-machine commerce.

Fog-based blockchain provides opportunities for verifying trustworthiness, security, and privacy. One of the drawbacks of the decentralized system is how to trust that the peers are actually trustworthy to deal with. Through signing interactions between peer devices, it is possible to dispute the activities of peers, based on trust levels. This enables activities such as peer maintenance, self-maintenance, and servicing, to occur without human intervention. Integrating blockchain and fog technologies can facilitate inter-device agreement (trustworthiness) by using public key infrastructure settings deployed in the blockchain structure to prove the identity of each device before they can transact. This can be achieved by having the fog operate on top of the blockchain backbone.

Blockchain, combined with fog computing, can create a robust, efficient, and highly competitive marketplace, where the best offer in a given fog takes it all. This can be achieved by determining all possible factors, such as time and energy on top of the cost, to determine the most appropriate service or product.

Other opportunities are found in extending secure real-time services of the internet of things, such as analytics and always-available services, anywhere, anytime. Devices requiring different services, such as computational power, storage, etc. can easily connect to the blockchain, and identify other devices that are in need of given services, so that they can trade with each other. Let’s say device A has dormant storage that it would not be likely to use in the near future, it can trade its surplus storage

space for additional processing power to execute a given task nearby, such as real-time analytics.

Blockchain technology and fog attract wide-ranging use cases, from connected things, industry, agriculture, and finance, to health services. There is no doubt that blockchain adds substantial value to the internet of things. Big data machine learning, and other series' of new information technology innovation which have appeared in recent times, are likely to take some time to mature. This is because of problems associated with blockchain adoption which must be alleviated among them first. These challenges include:

- **Scalability:** the spread of the number of users as a result of the upcoming number of use cases created in the IoT environment, users and devices which need to use blockchain technologies, is gradually rising, and scaling the technology to support users is overwhelming. As a result, blockchain networks experience slowed transactions and higher fees charged per transaction. Proposals to improve on scalability have appeared recently, but are still highly varied, and are likely to take a significant amount of time to mature. In addition, scaling methods may need to be verified and thoroughly vetted before implementation into the ledgers. Scalability concerns need to be well addressed before blockchain can be adopted on a wide scale.

- **Energy consuming consensus mechanisms**: The majority of consensus mechanisms rely on processing power, which has a significant impact on consumption of energy. Implementing them in the internet of things and the fog tends to be costly. With current concerns about global energy consumption, fog-blockchain may need to use green energy harvesting methods and energy saving consensus algorithms, such as proof-of-stake, etc., to sustain computation in future technology.

- **Inept technological design:** The fog technologies, and blockchain are still in the infant stage of development, facing a number of issues, such as vulnerability due to their coding, to achieve components such as smart contracts. In addition, quite a substantial amount of data is involved within each transaction yet not all is essential, and this makes the network slow. Mechanisms for

optimizing network activities to achieve efficiency in operation are not yet widespread.

- **Privacy and security:** These are still open issues. The fact that the design of fog-blockchain is publicly visible, means that information such as financial records, government secrets, or patients' information, which ought to be preserved, need not be public. This may necessitate that some part of a transaction remains private to the ledger, so as to limit access to data contained therein, particularly in a situation where a miner or a group of miners control more than 50 percent of the mining power. The users are able to reverse the transactions they have confirmed, raising issues of security, although this situation is unlikely with a large network.

- **Costs of new innovation:** Fog-blockchains are a relatively new innovation which is difficult to integrate with legacy systems. Convincing stakeholders to become involved may take a considerable amount of promotion. However, blockchain technology and the fog combined, is an effective tool for reducing costs, improving efficiencies, reducing the fees associated with transferring value and services, and is stand-alone, streamlining operational processes.

5. Conclusion and Recommendations

In spite of the recent spread in crypto-currency, all thanks to blockchain technology, there are still different ways in which blockchain technology can be used outside the financial sector to build powerful solutions. Many business organizations are shifting their business models from the traditional set up of infrastructure, which has a very high initial cost, to buying cheaper cloud services from technology giants like Google, Amazon, Microsoft, etc. Nevertheless, cloud computing has its own weaknesses, such as unreliable latency, lack of location support, and being centralized. The fog can mitigate the weakness of the cloud.

This chapter presents the advent of the fog-cloud-of-things, and examines the application of blockchain technology in the building blocks of fog computing which attract the application of blockchain. The concepts underlying fog computing, the internet of things, and blockchain technologies, have been discussed at length. Our objective was to explore opportunities and challenges by providing important aspects of fog

computing in relation to blockchain technology, such as its architecture, the required key features, opportunities, and challenges. We further provide recommendations to open up future investigations.

We note that not all technologies are deemed fit for all situations, Nonetheless, the fog combined with blockchain paradigm is likely to propel the internet of things into new directions, including rural and urban use cases alike.

As governments, organizations, and business entities, scientists and technologists, and academia, are striving to push data-driven economies further to maturity, amidst competition and scarce resources, the fog cloud of things-blockchain can offer a platform for the IoT that is distributed, always available, trusted, and secure.

It is important for both standard organizations and governments to rethink policies relating to new technology. The pace at which technology is developing today may create a gap between application and policy. Therefore, apart from international standard organizations, individual governments should look at roadmaps to identify issues related to use-cases relevant to their situation, rank the order of standards development activities, and pinpoint technical issues, including any support that is needed to achieve technological progress. Each government has its own technological requirements. Blending these to fit within international arrangements may create disparity in many ways, creating gaps in adoption of the technology. Creating standards at either local or regional levels will help to increase collaboration within applications development, will help development itself, will further the sharing of proof of concepts, and spread the sharing of blockchain solutions before integrating them into a comprehensive framework.

There is a need to bridge the gap between users, technical people, and business people, so as to create an understanding of blockchain and its applications. It is common to associate blockchain applications to bitcoin, or other cryptocurrencies. In many situations, the feeling that new technology is not worth investing in is a huge drawback. It causes many businesses to miss out on the benefits of that technology. There is a need for a bridge between technologists and businesspeople to ease the implementation of any new technology, such as blockchain in related use cases. Technology investment needs to be translated into business products. The performance of blockchain infrastructure requires an

amount of fine-tuning, to run on systems which have low processing power. This, in essence, requires a lot of effort.

Being a new technology of slightly a decade, blockchain infrastructure is yet to mature, it is power-hungry and may not be applicable in a rural world where electricity is lacking. In situations where power may be available, the cost of running the infrastructure may be quite high. Some flocks maintain that the energy consumption will be unsustainable, and this may require new designs in the consensus mechanism.

References

[1] S. Asur and B. A. Huberman, "Predicting the Future With Social Media," 2010.

[2] Manuel Castells, "The Impact of the Internet on Society: A Global Perspective - MIT Technology Review," MIT Technology Review, 2014. [Online]. Available: https://www.technologyreview.com/s/530566/the-impact-of-the-internet-on-society-a-global-perspective/. [Accessed: 16-Dec-2018].

[3] Mary Aleksandrova, "IoT in Agriculture: 5 Technology Use Cases for Smart Farming (and 4 Challenges to Consider) : Eastern Peak," 2018. [Online]. Available: https://easternpeak.com/blog/iot-in-agriculture-5-technology-use-cases-for-smart-farming-and-4-challenges-to-consider/. [Accessed: 16-Dec-2018].

[4] Mutwalibi, Nambobi ; Md. Shahadat, Hossain, Khan; Adam, A. Alli, "Big Data: Prospects and Applications in the Technical and Vocational Education and Training Sector," in Data analytics : concepts, techniques and applications, 1st ed., Taylor Francis, 2018.

[5] C. Zhang and J. Sun, "Privacy and Security for Online Social Networks: Challenges and Opportunities," no. August, pp. 13–18, 2010.

[6] B. Negash, A. M. Rahmani, P. Liljeberg, and A. Jantsch, "Fog computing fundamentals in the Internet-of-Things," in Fog Computing in the Internet of Things: Intelligence at the Edge, 2017, pp. 3–13.

[7] I. Stojmenovic and S. Wen, "The Fog Computing Paradigm: Scenarios and Security Issues," Proc. 2014 Fed. Conf. Comput. Sci. Inf. Syst., 2014.

[8] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, "Fog computing: A platform for internet of things and analytics," Stud. Comput. Intell., vol. 546, pp. 169–186, 2014.

[9] Helder Antunes, "Blockchain and Fog: Made for Each Other," cisco blog, 2018. [Online]. Available: https://blogs.cisco.com/innovation/blockchain-and-fog-made-for-each-other. [Accessed: 19-Oct-2018].
[10] P. K. Sharma, M. Y. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," IEEE Access, vol. 6, pp. 115–124, 2018.
[11] L. Zhou, L. Wang, Y. Sun, and P. Lv, "BeeKeeper: A Blockchain-Based IoT System with Secure Storage and Homomorphic Computation," IEEE Access, vol. 6, pp. 43472–43488, 2018.
[12] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," IEEE Access, vol. 6, pp. 32979–33001, 2018.
[13] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog {Computing} and {Its} {Role} in the {Internet} of {Things}," in Proceedings of the {First} {Edition} of the {MCC} {Workshop} on {Mobile} {Cloud} {Computing}, 2012, pp. 13–16.
[14] D. Ivans, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything," 2011.
[15] H. C. Hsieh, J. L. Chen, and A. Benslimane, "5G Virtualized Multi-access Edge Computing Platform for IoT Applications," J. Netw. Comput. Appl., vol. 115, pp. 94–102, 2018.
[16] Z. K. A. Mohamed and E. S. A. & Ahmed, "Internet of Things Applications , Challenges and Related Future Technologies," WSN World Sci. News, vol. 62, no. 2, pp. 126–148, 2017.
[17] P. Guo, B. Lin, X. Li, R. He, and S. Li, "Optimal Deployment and Dimensioning of Fog Computing Supported Vehicular Network," in 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 2058–2062.
[18] S. Madakam, R. Ramaswamy, and S. Tripathi, "Jcc_2015052516013923," no. May, pp. 164–173, 2015.
[19] X. M. Chen, N. S. Yang, and Z. X. Guan, Analysis to the stress and strain structures of mode I 3-D crack in elastic-plastic state, vol. 3, no. 3. 1990.
[20] "2017 International Conference on Information and Communication Technologies, ICICT 2017," 2017 Int. Conf. Inf. Commun. Technol. ICICT 2017, vol. 2017–Decem, no. December, 2018.
[21] J. Lianghai, B. Han, M. Liu, and H. D. Schotten, "Applying Device-to-Device Communication to Enhance IoT Services," IEEE Commun. Stand. Mag., vol. 1, no. 2, pp. 85–91, 2017.
[22] M. Bennis, M. Debbah, and H. V. Poor, "Ultra-Reliable and Low-Latency Wireless Communication: Tail, Risk and Scale," 2018.

[23] M. Höyhtyä, O. Apilo, and M. Lasanen, "Review of latest advances in 3GPP standardization: D2D communication in 5G systems and its energy consumption models," Futur. Internet, vol. 10, no. 1, 2018.
[24] U. Uyoata and M. Dlodlo, "Relay Assisted Device-to-Device Communication: Approaches and Issues."
[25] J. Lianghai, B. Han, M. Liu, and H. D. Schotten, "Applying Device-to-Device Communication to Enhance IoT Services," IEEE Commun. Stand. Mag., vol. 1, no. 2, pp. 85–91, 2017.
[26] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," 2015 Internet Technol. Appl. ITA 2015 - Proc. 6th Int. Conf., vol. 113, no. 1, pp. 219–224, 2015.
[27] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved," IEEE Internet Things J., pp. 1–1, 2018.
[28] J. Miranda et al., "From the Internet of Things to the Internet of People," IEEE Internet Comput., vol. 19, no. 2, pp. 40–47, 2015.
[29] J. Mendling et al., "Blockchains for Business Process Management - Challenges and Opportunities," ACM Trans. Manag. Inf. Syst., vol. 9, no. 1, pp. 1–16, Feb. 2018.
[30] A. Wright and P. De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia," Ssrn, 2015.
[31] X. Chen, L. Jiao, W. Li, and X. Fu, "Efficient Multi-User Computation Offloading for Mobile-Edge Cloud Computing," IEEE/ACM Trans. Netw., 2016.
[32] A. V. Dastjerdi and R. Buyya, "Fog Computing: Helping the Internet of Things Realize Its Potential," Computer (Long. Beach. Calif)., 2016.
[33] M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," IEEE Internet of Things Journal. 2016.
[34] Y. Yuan and F.-Y. Wang, "Blockchain and Cryptocurrencies: Model, Techniques, and Applications," IEEE Trans. Syst. Man, Cybern. Syst., vol. 48, no. 9, pp. 1421–1428, Sep. 2018.
[35] S. Brakeville and B. Perepa, "Blockchain basics: Introduction to distributed ledgers," Int. Bus. Mach., 2016.
[36] B. Laurie and R. Clayton, "Proof-of-Work Proves Not to Work," 2004.
[37] Pawel Szalachowski, "Towards More Reliable Bitcoin Timestamps," arXiv:1803.09028v2, vol. 1, no. 1, 2018.

[38] K. Rilee, "Understanding Hyperledger Sawtooth — Proof of Elapsed Time," Medium, 2018. [Online]. Available: https://medium.com/kokster/understanding-hyperledger-sawtooth-proof-of-elapsed-time-e0c303577ec1. [Accessed: 23-Jan-2019].

Authors Biography

Adam A. Alli, is a PhD. in Computer Science and Engineering fellow at Islamic University of Technology (IUT), Board Bazar, Gazipur-1704, Bangladesh. He received his MSc. in Computer Science (2008) at the University of Mysore India, B.Sc. in Computer Science (2002) at Islamic University in Uganda. He also received a postgraduate diploma in Management and Teaching at Higher Education (2015) at Islamic University in Uganda, and a Graduate Diploma in ICT Leadership and Knowledge Society (2013) at Dublin City University through the GeSCI program. He was Dean Faculty of Science at Islamic University in Uganda from 2011 to 2016. He is a lecturer of Computer Science and Engineering at both Islamic University in Uganda and Uganda Technical College (UTC) Bushenyi. He is a lead researcher for Islamic University in Uganda ICT4D group.

Mugigayi Fahadi is a Research Member at the Department of Technical and Vocational Education (TVE); Islamic University of Technology (IUT), Board Bazar, Gazipur-1704, Bangladesh. He is a final year Masters' student specializing in computer science and Engineering. He received his B.Sc. in Information Technology with a First-Class Honors (2016) at Islamic University in Uganda. Upon Graduation, he was recruited as a graduate internee at United Bank for Africa Uganda Plc where he was later promoted to Relations' Officer. While pursuing his B.Sc. he was working as a mobile Application developer at Hansu Mobile and Intelligent Innovation Ltd.

Atebeni Cherotwo, is a Master in Science and Technical Education (MSc. TE) specializing in Computer Science and Engineering at Islamic University of Technology (IUT), Board Bazar, Gazipur-1704, Bangladesh. He received his Diploma in Computer Science and Information Technology (DCIT) in 2010 and Bachelor of Information Technology (B.I.T) in 2016, both from Islamic University in Uganda. Currently, he is a computer Lab Officer and a member of ICT4D in the same institution.

CHAPTER FIVE

A NEW ERA OF PROJECT MANAGEMENT USING BLOCKCHAIN TECHNOLOGY

TAHMINA RASHID[1], MUNIR A. SAEED[2] AND MOHIUDDIN AHMED[3]

[1]Faculty of Arts and Design, University of Canberra, Australia
[2]School of Engineering and IT, UNSW Canberra, Australia
[3]Academic Centre of Cyber Security Excellence, School of Science, Edith Cowan University, Australia

Abstract

Blockchain technology is being embraced in a wide range of application domains. Although usage is mostly in the financial sector, the effectiveness of this emerging technology is being investigated in other domains as well. In this chapter, we are interested in exploring the effectiveness of blockchain technology for project management (PM). Project managers can use blockchain technology to enhance the performance of any project. Blockchain can be used to communicate with all participants in order to define requirements, scope, budget, deadlines, and deliverables. Additionally, blockchain will identify, verify, and validate, all transactions. This technology can help simplify any issues that involve reconciliation, arbitration, or intermediation. The chapter will help both academics and industry practitioners to gain more understanding of the benefits of using blockchain for project management.

Keywords: Project management, contracting, procurement, construction, project manager.

1. Introduction

Blockchain is a technology used by digital currencies such as bitcoin and Ethereum. Bitcoin was introduced in 2009, and now it is evident that private businesses and public sector organizations are fast adopting blockchain technology. [1] Blockchain technology is inherently designed to establish a network based on trust. This technology is perfectly suited to cases, where only trusted participants are authorized to write records. Blockchain is a very promising technology and it is pertinent to explore how this this emerging technology can be employed in project management.

In project management, running projects efficiently and effectively is one of the challenges, as project success is based on completing on cost, on time, and meeting scope specifications. Referring to the CEO of Venturing and Emerging Brands (VEB), there is a visible absence of a platform to manage projects efficiently, but blockchain offers a promised fundamental and qualitative platform, which can serve project management in the future. [1] Therefore, blockchain offers possibilities to improve project governance and minimize bureaucracy. Project management literature and standards frequently mention the significance of developing project deliverables on time, meeting cost estimates, and scope specifications. [2]

Blockchain offers great potential for managing contracts within project management. Contract management falls into the procurement knowledge area, which is one of the ten key knowledge areas in project management. [3] Before we discuss how blockchain can improve contract management, it is pertinent to understand procurement, and its role, particularly in the construction industry.

PMBOK defines procurement management as '…the processes involved in the acquisition of goods and services…' and similarly, APMbok defines procurement as a process through which services and products can be acquired. Kathy Schwalbe defines procurement as acquiring or procuring goods and services for a project outside the organization. [4] However, Walker and Rowlinson argue that project procurement can take place within the organization, and be outsourced to an external entity. [5] The decision to procure internally or externally is dictated by project typology, the project sponsor's expectations from the project, and what constitutes value from the outcomes of a project. Supporting the justification for procuring outside the organization, Schwalbe states that, as the world is getting more and more competitive and global, project managers recognize

the benefits of procuring from the market. [4] Since the role of a project manager entails doing what is in the best interest of the project, and the project organization, procuring goods and services from outside the organization becomes a logical conclusion. Kloppenborg et al. [6] add a little more dimension to procurement, by saying that procurement management is acquiring or purchasing products, services, and contract management. The UN considers public procurement as a process, which encompasses acquiring goods and services, civil works, and all the stages of the contracting process. Public procurement should not be considered a process that centers on a supporting role, in fact it includes the strategy and policy of an organization, its methods, procedures, and personnel as well as the organization itself. [7]

The endeavor to develop a comprehensive definition of procurement seems to have been dominated by the construction industry. [5] However, Mohsini and Davidson argue that other sectors of the economy, such as the manufacturing, automobile, shipbuilding, and aerospace industries, have adopted forms of procurement similar to the construction industry. [8] There has been a debate over an appropriate and comprehensive definition of procurement. In this regard, Mohsini and Davidson write, the CIB commission adopted an initial definition of procurement as "the act of obtaining by care or effort, acquiring or bringing about." [5] They further write that such a definition was expected to enhance the conceptualization of procurement and increase an awareness of the challenges associated with current practices, in addition to establishing new strategies. Lenard and Mohsini attempted to refine the definition by defining procurement as the acquisition of new building or space within buildings, which may comprise directly buying, renting or leasing from the open market, or through custom-designed and built facilities in order to meet required needs. [9] Masterman states that the CIM Commission, after a debate over the definition in 1997, came with up with an improved definition of procurement, according to which, "procurement is a strategy to satisfy client's development and or operational needs in order to provide built facilities and a discrete lifecycle." [10] Therefore, the commission has attempted to offer a definition which, in fact, encompasses the entire lifecycle of building. The current procurement systems are divided into three main categories, [11] such as:

- Separate and co-operative procurement systems;
- Integrated procurement systems- design and build and its variants;
- Management-oriented procurement systems.

1.1 Chapter Roadmap

The rest of the chapter is organized as follows: Section 2 reflects the historical background of procurement systems. Section 3 discusses procurements systems in detail. Section 4 reflects procurement and value, followed by blockchain and contracting in section 5. The chapter is concluded in section 6.

2. Historical Background of Procurement Systems in the Construction Industry

Providing the historical background on the evolution of procurement systems particularly within the construction industry, Masterman writes that, before the start of WWII, the majority of construction works were carried out through conventional procurement methods, which were in vogue for a century and a half. [11] However, after the end of WWII, some of the procurement choices were imported from the US, and the willingness of client organizations to experiment with new methods heralded the emergence of new procurement methods. Masterman identifies the following three phases in the evolution of procurement systems in the UK construction industry: [11]

1945-1972 (predominantly conventional methods)

During this post-war period, the UK experienced continuous economic growth, and conventional methods were predominantly employed, however, there is evidence of a small number of projects completed through non-conventional methods as well. [11]

1973-79 (the initial advent of non-conventional systems)

This era was marked by recession, which was further worsened by the oil embargo by the major oil producers. The UK economy suffered from high inflation, which was in fact the residual effect of the post-war era of bullish economic activity, which lasted from 1945-1972. Masterman mentions various reports on the construction industry in the UK, which found that the procurement systems used by the public sector were not appropriate in the light of prevailing economic circumstances. [11] During this period, though conventional procurement systems were predominantly used, there was a move towards other methods, such as management contracting, and design and build.

1980- to 1992 (a significant move towards non-conventional systems)

The third period was marked by the post-recession trends towards recovery, which resulted in structural changes in the construction industry in the UK. In this phase, conventional systems were mostly employed, but there was significant transition towards the use of design and build and various other forms of management contracting. [11]

3. Procurement Systems

3.1 Traditional/Conventional Procurement Systems

According to Masterman, [11] the conventional/traditional method of procurement was in use during the 18th and at the start of the 19th centuries, when clients hired craftsmen individually, and they were normally supervised by a master mason or surveyor. In traditional procurement systems, the defining characteristics were that the design and construction were two discrete processes. These two entities retained their degrees of separation, even in other variants of the conventional procurement systems. Mohsini and Davidson [8] state that the traditional procurement approach is based on the separation of various phases, such as design, development, tendering, contract and construction delivery. In this procurement route, design is nearly complete before calling the tenders, however, in practice, certain aspects of the design are deliberately not finalized before the tender, so that some improvements can be made during the delivery. [8] The unfinished design opens up a window of opportunity for contractors to make claims for extras, which consequently leaves the client at the mercy of contractors. According to Mohsini and Davidson, [8] the reasons clients still opt for this procurement choice, are possibly the degree of familiarity with the system, and the initial appeal of the cheapest price. Dalrymple et al. [13] argue that the traditional procurement systems lack value for money. Mohsini and Davidson [8] problematize the existence of poor quality of relationships between project teams and delivery systems, as the traditional system, the authors argue, disconnects the contractor from the design phase, therefore the opportunity to benefit from a contractor's knowledge, and the information of constructability is lost. Mohsini and Davidson [8] suggested that the constructor can provide useful advice on how to effectively meet design requirements in an effective manner, in terms of cost and time.

According to the Procurement Systems Manual of the NSW government Public Works department, [12] where a single contract covers the entire project, design and build is the most suitable option. The Manual says that single contract is the most suitable for small works, and the majority of public works, such as schools, where splitting the work activities is either not required or is not effective. It is the most simple, and the Manual recommends this procurement choice should always be considered. The Manual recommends single contract as a delivery system, where a client wants to be certain about the end costs at the start of the construction. However, this delivery system requires adequate time to finalize the design and other documentation before the commencement of construction. The Manual also recommends a single contract system where the client's skills and resources for construction management are limited, or non-existent. The single contract also transfers those risks, which are normally associated with the coordination of separate contract packages, to the contractors. While identifying the disadvantages of a single contract delivery system, the Manual writes that the client misses the opportunity to fast track the construction, particularly when 'construct only' or a DD&C contract system is adopted. This delivery system also results in the loss of control over the design, if the D&C contract system has been adopted. The single contract delivery system also constrains the client's ability to make any changes in the status of the principal or the contractor. Among other disadvantages of a single contract, the Manual includes reduced flexibility in cash flow management, and it requires immediate commitment to the full project. It also requires a finalized 'client brief' before the start of construction, and later changes by the client are not cost-effective.

The multiple contracts delivery system is adopted where a project is divided into various multiple contracts. This delivery system offers decision makers various combinations of contract systems. The multiple contracts system allows a project to be split into independent entities, therefore, it makes staging possible. This delivery system perfectly suits where separate contracts are required, because of the project complexities. The project can be broken into trade packages. This system allows compression by permitting construction to start at the early stages, as it does not require finalized design or other documents before the beginning of the construction. As compared to a single contract, the multiple contracts system offers control over cashflow, the flexibility of redesigning cost effectively, and the ability to accommodate changes. The multiple contracts system supports response to technological changes, and effective control over the design and construction quality, by permitting

direct control over the selection of the work and trades contractors. It also facilitates control over the pace of work, in accordance with the cashflow requirements of the client. As far as the disadvantages of the multiple contracts delivery system are concerned, the Manual states that the risk of coordination rests with the principal, and the client may be tempted to request changes, because of the flexibility offered by the delivery system. There is an increased chance of discrepancies between the packages.

The Manual states that the period contract is not strictly a delivery system, as it is employed mostly in maintenance programs. These contracts are generally trade-based and contracts are required for a specific work at the tendered rates, whenever the required work comes up.

In the direct labour delivery system, the principal hires and supervises the tradesmen and the labour directly. This type of delivery system was employed in public sector projects, but its use is negligible these days. [12]

3.2 Construct Only

In this contract type, the principal carries out the detailed design for the entire project, or a part of it. The design can be built-in-house or can be assigned to consultants. This strategy is adopted for the following reasons:

- The optimal design can be completed before involving the possible builder and or sub-contractors;
- The principal is able to control the development of detailed design and documentation and the construction, besides enjoying the freedom to engage the consultants, who are solely responsible to the principal;
- It allows adequate time to complete a detailed design before the start of the construction work.

According to the NSW government Public Works Manual [12] ‘construct only’ enables the principal to contribute considerably to the conceptual design, and identify the performance criteria. By having a fully developed design, the ‘construct only’ procurement root increases the probabilities of a quality product. A fully developed design before the tender reduces the design-related risks to the principal. A fully developed design may help to get realistic price estimates. The developed design means a reduced amount of work for the bidders, and it may attract a larger number of bidders, thus enhancing competition and the possibilities of competitive

pricing. The NSW government's Public Works Manual states that the 'construct only' procurement choice may not allow fast tracking the project, as it requires a longer lead time to prepare design and documentation for tendering. If the principal lacks the necessary skills in-house, it might lead to making mistakes in the documentation, which might result in possible claims.

3.3 Design and Construct (D&B)

Masterman [11] argues that design and build has become a popular procurement choice in the UK. Masterman claims that design and build is possibly the oldest procurement method, and is still being employed in the UK. This method, he argues, offered increased efficiency and low costs in the wake of growth in some sectors of the economy in the UK during the 1960s, which led to the adoption of the design and build method by the public sector. Masterman [11] further writes that, in the wake of 1973-74 oil embargo, the increase in the rate of borrowing and inflation, caused by the post WWII economic activity boom, required projects to be started and completed quickly. He argues that, at the same time, due to poor performance, clients' dissatisfaction with conventional methods increased. In these circumstances, design and build offered the integration of design and construction, and that too, with the attractive cost savings and fixed price lump sum reimbursement tenders, became the market favorite. [12] Explaining the design and build procurement method, Masterman [11] writes that it is an arrangement in which a contracting party takes complete responsibility for the development of a custom-built design, and its construction. This type of procurement strategy has three main characteristics: the responsibility of design and construction rests with one organization; payment is generally based on a fixed price, and is made on lump sum basis; and the project is tailored to meet the requirements of the client. [11] Akintoye [14] states that design and build is more popular with the private sector (21%) than with the public sector (12%) of the workload in the UK construction industry. In their survey of 52 construction firms, carrying out 25% of the total output of the UK construction industry, Akintoye argues, the survey results do not support the criticism of D&B that this procurement choice is not suitable for complex projects. To support this, Akintoye refers to the use of D&B in the private sector for health facilities and refurbishment civil engineering projects. However, the author admits that the use of D&B has been in decline for refurbishment projects, not because of some inherent weaknesses, but rather due to the

challenges of exactly defining client requirements, the difficulties of assigning risk, and the lack of clarity of the brief. [14]

3.4 Design Development and Construct (DD&C)

According to the NSW government Public Works Manual, [12] in this procurement choice, the principal prepares the design of the concept, and the performance specification, which can then be done in-house, or by external consultants. Then the development of the detailed design and construction work is carried out through a contract.[12] This procurement choice is adopted by those clients who have developed the design concept and related details, thus enabling them to avoid the challenges of coordination and the associated risks of construct-only. The Manual[12] argues that this procurement route also saves the client from having to have the in-house skills for developing the design, as required in 'construct only' strategy. According to the Manual, DD&C requires the client to have the design brief defined and developed. This way, the client retains control over the conceptual design. According to the Manual, this procurement choice has the following advantages:

- The principal can contribute to the conceptual design and identify the performance criteria;
- The responsibilities of the design details and coordination can be transferred to the contractor, therefore reducing the risks to the principal and consequentially, the principal enjoys savings from not requiring the resources and skills to develop the design;
- DD&C also offers opportunities for saving through faster and efficient construction, and it also enables the contractor to modify the design details to suit preferred construction methods.

Among the disadvantages, the Manual [12] includes the high costs of preparation for tenders, which might result in lack of interest by the bidders, consequently leading to a lackluster competition. This type of contracting may cost more to the client, where variations are requested.

3.5 Total Package Options, BOO, BOT, BOOT

According to Mohsini and Davidson, [8] the traditional procurement system category is based on fixed cost options. In the total package option procurement strategy, the project needs of the client are fulfilled by an organization which contracts to carry out phases such as design, build,

operate, own for a specific time, and then transfer the facility to the client. These packages are known as BOO, BOT and BOOT. [8] In this abbreviated term, B stands for build, O means own and/or operate, and T stands for transfer. The BOT procurement route is based on the conventional wisdom that risk should be transferred to a contracting party (mostly in the private sector) who is more capable of managing associated risks. [5] [15] According to Walker and Smith [16] the main objective of a BOT package is to acknowledge and offer an apparatus to manage the associated risks. The BOT packages are more suitable for infrastructure projects, and not fit for small ones, however, Walker and Smith state that, increasingly, governments have resorted to the BOT family for projects such as hospitals and prisons. [8] In BOT, the investing party takes on the responsibility to carry out all phases from design to operation, therefore, the associated risks are also managed by the same organization. However, Walker and Rowlinson [5] have identified some failures in projects based on BOO/BOT/BOOT, wherein they argue that failures were caused by lack of trust and poor communications on the part of contracting parties. In this regard, they particularly mention the Bangkok Second Stage Expressway. Buljevich et al. [17] have identified the success factors of the BOT family, such as strong relationships with the host governments, organized resource allocation, efficient funding, a high rate of confidence among investors, and access to markets for raising funds and the transfer of ownership. Chen et al. [18] state that BOT, with higher levels of private participation, promises efficiencies to both private and public sectors. However, they argue that the BOT procurement system requires a favourable political, economic, legal, and institutional environment. In this regard, Chen et al. [18] refer to UNIDO, which states that BOT projects are complex in nature, both financially and legally, and entail time-taking processes, such as negotiations and proposal development. The authors believe that internationally-practiced BOT procurement arrangements need to be customized to fit into the existing political, economic, and legal environment in China. However, they appreciate the fact that, in order to provide a supportive climate for BOT as a procurement system, a process of reforms is underway in China. The application of BOT as a procurement choice is replete with confusions and snags, not only for the investors but also for government agencies in China. Therefore, the authors believe that, due to the prevalent confusion, BOT-based projects have encountered failures in China, and they suggest the elimination of discouraging environments. According to Chen et al., [18] the China-specific drivers and impediments of the BOT procurement method-based projects in China are as follows:

➢ **Drivers for BOT family procurement routes**

- The need for capital to develop infrastructure
- The need for advanced technology
- The need for management skills
- Trends towards the commercialization of infrastructure services
- Promotion of reforms in financing and infrastructure investment

➢ **Impeding factors for BOT family procurement routes**

- Legal system is weak and complicated
- Intricate approval processes
- Restrictive regulatory regime for new entrants to the market
- Lower market prices for infrastructure products and services
- Creditworthiness of local utilities
- Local government, and its lower tiers, do not have direct interest in projects
- Restrictive currency administration

3.6 Public Private Partnership (PPP)

The Singaporean Ministry of Finance states that PPPs in Singapore have helped the public sector to get value for money in delivering public services. [19] Besides, PPPs have provided opportunities to the private sector to innovate and develop efficient solutions. They claim that this procurement route has enabled the private and public sectors to effectively provide public services. Identifying the drivers for the adoption of PPPs, Chowdhary et al. [20] argue that some countries have resorted to PPP due to fiscal deficit, budgetary pressures, and gaps in demand and supply, and others have adopted PPP for efficiencies in operation, technological innovations, and management skills of the private sector in the provision of public services. Similarly, Raisbeck et al. [15] state that PPP as a choice of procurement, is on the rise in Australia, as the Australian government plans to spend $320 billion on infrastructure facilities in the next decade. In order to demonstrate the effectiveness of PFIs, Raisbeck et al. [15] refer to a study conducted by the National Audit Office (NAO) in the UK, which shows that 76% of PFI projects were completed on time, and 78% were completed on budget. Whereas, according to NAO reports, projects procured by employing traditional procurement methods were 70% completed on time, and a mere 27% were completed on budget. Cambridge Economic Policy Associates [21] reported that Scottish PPPs

have performed well, and similarly, Kakabadse et al. [22] also conclude that PFIs are doing well in the UK. However, the report commissioned by the UK Association of Charted Accountants criticized the PFI, arguing that the real beneficiaries of PFIs are finance providers, and, to some extent, the private sector service providers, rather than the public sector. Raisbeck et al. [15] argue that the Australian projects procured through PPPs have shown higher cost efficiencies as compared to traditional methods. Supporting their claim, Raisbeck et al. [15] write that the cost overruns were only $58 million for PPP projects, of $4.9 billion contracted value, whereas they argue that the projects procured through traditional methods, with a contracted value of $4.9 billion, have suffered cost overruns to the tune of $673 million. [15] However, Raisbeck et al. [15] did not detect any statistical difference in terms of time overruns between the performance of PPPs and traditional projects. They point out that projects of smaller size, procured through traditional systems, were completed early, but that as project size increases, the traditionally procured projects start suffering from time overruns. Therefore, in the light of the analysis of Raisbeck et al., [15] it can be concluded that the PPP method of procurement is more effective and efficient in cost and timeliness in large projects, whereas, the smaller-sized projects, procured through traditional methods, benefit in terms of early completion. Raisbeck et al. [15] argue that, due to the absence of global benchmarking for PPPs, the comparison of Australian PPPs with projects procured through PPP routes in other countries, is challenging. Therefore, Raisbeck et al. [15] support the need for standardized metrics to measure the projects procured through PPPs at global level. Australian decision makers should have the option of procuring through PPPs, particularly when finances are limited and project size is larger. [15]

3.7 Turnkey

Masterman [11] states that the private sector in the US extensively used the turnkey procurement method to build facilities such as oil refineries and power stations during the early 19th century. Masterman also points out that the turnkey method was employed to build similar facilities in the UK as in the US, but that its application has been insignificant. Walker et al.[9] argue that the turnkey method allows the supplying organization to finance the project, in addition to designing and constructing responsibilities. Walker and Hampson [8] write that the turnkey method in a way resembles BOT, but in turnkey, the contractor does not undertake to operate the facility. Masterman [11] states that turnkey, as its name

indicates, is a procurement route in which a single contractor takes the responsibility for the entire process, from the design to final completion of the facility, until such time as the facility is ready to be operational at the turn of a key. According to Lenard and Mohsini, [9] through the turnkey method, the client pays the contracting organization on the completion of commissioning and testing of the facility. They state that the turnkey method suits those clients who wish to make payment only when the facility is handed over to the client, due to financial or tax gains. [9]

3.8 Management Contracting (MC), Construction Management (CM) and Project Management

According to Mosey, [23] management contracting (MC) and construction management (CM) are two procurement methods which allow the early involvement of the contractor. The early appointment of the contractor is aimed for at the start. Masterman [11] argues that management-oriented procurement methods have been adopted by commercial clients who wish to start and complete their projects early, and these objectives could not be achieved by employing traditional methods. Masterman [11] includes the design and manage (D&M) method in the management suite of procurement choices which comprises MC and CM. According to Francis and Sidwell, [24] the management-oriented family of procurement methods brings the contractor on board early, thus it increases the crucial role of constructability advice in the development of design. Sidwell and Ireland [25] state that, in CM, the contractor plays the role of a consultant to provide useful input on the design issues and possible building methods. Mosey [23] identifies the subtle difference between MC and CM, suggesting that, in management contracting (MC) the management contractor procures a series of work packages. Though the management contractor enjoys the authority of a main contractor, this authority is limited only to recoverable amounts from the defaulting package contractor. In construction management (CM), the client directly awards the packages to sub-contractors, and the consultant construction manager owes a professional duty of care to the client, just like other consultants.

Mosey [23] writes that project management entails the appointment of a professional as a project manager, who will appoint design consultants and contractors to conduct the construction of the facility. This procurement route is suitable for large facilities and engineering projects. The role of the project manager is to coordinate the design and construction tasks, and ensure that the project is completed within cost, time, and quality

constraints. However, Love et al. [26] do not consider project management as a procurement method, as project management can be applied to any procurement method. Similarly, Bennett [27] does not consider project management as a procurement choice either. Love et al. [26] argue that project management means only that a client has hired the services of an agent to carry out coordination and supervision activities. Walker et al. [9] state that PM as a procurement system emerged in the 1960s and 1970s. The PM team takes responsibility for coordination with the design team, and interacts with those who are responsible for delivering the work packages. However, the PM team maintains a safe distance while interacting with the design team and the construction team.

4 Procurement and Value

Despite variations in definition across the industries, there seems to be a general consensus on the primary objective of the procurement process - value generation. Walker et al. [9] consider value generation as the main purpose of the project management exercise. They argue that project teams generate value for all stakeholders, and a sustainable procurement process offers opportunities for value generation for all parties, thus leading to a win/win, rather than win/lose outcome. Value seems to be the ultimate objective of the entire exercise of project management, which includes procurement as an important process. What does value mean for project stakeholders? Value has been described as tangible and intangible expectations. The customer's delight is a matter of prime importance, and delight is achieved by exceeding customer expectations through excellent service. [28] Walker et al. [9] consider value as going further than fitness for purpose (tangible); rather their conception of value comprises intangible elements, such as quality of relationship, leadership, trust, and culture. The level of customer delight and value depends on how effectively these intangible expectations are met. [9] However, in their pursuit of customer delight and value, the authors do not lose sight of the significance of ethics and governance or the five important principles in the procurement process; value for money, ethics, competition, transparency, and accountability. [29] Walker et al. [9] emphasize the importance of incorporating value into the very fabric of the procurement process.

5 Blockchain and Contracting

Effective procurement and contract management warrants successful communication. Medina [30] states that a project manager is required to communicate with all stakeholders in order to define project scope, budget, timelines, and deliverables. Blockchain can help the project manager to identify, verify and validate transactions. Medina [30] further argues that effective cost management is one component of the iron triangle of scope, time, and cost, on which the project success was traditionally based. A major part of project expenditure is spent on labor costs, and data on how much time is spent by the project team to complete project tasks will be recorded on a long-term basis. This data can be shared with partners, and can be shared with trusted partners using blockchain technology, which allows access to authorized and trusted personnel.

This data can be employed to monitor project members working on different projects, ensuring that distributed team members allocate the required time to a given project, and denying the possibility of over-allocation of time by shared team members. Freelancing has become a popular way of contracting, particularly in the software development industry. Freelancing, where it involves distributed team members, also brings in new challenges of signing contracts and making payments, as the deliverables are completed by freelancers anywhere in the world. Blockchain offers solutions to this emerging pattern of workers in project management. Medina [30] states that smart contracts, a term first used by the cryptographer Nick Szabo in 1997, are now being employed. Smart contracts based on blockchain are contracts just like the standard contracts in the real world, except that these are digital. Smart contracts have the capability to hold payment till a deliverable has been handed over, or a project objective is achieved. [30] Smart contracts can prove to be useful in public sector projects where payments are mostly required to be made before the end of the financial year. There are some solutions offering smart contracts, such as Upwork, specially targeted at freelancers (www.upwork.com). A similar platform, particularly focusing on the IT industry is Alehub, which claims to usher in a new era of project management. According to *Bitcoin Magazine*, Alehub was launched in 2017, and is a blockchain-based digital platform that helps businesses with the identification and approval of contract partners. Alehub claims that that the platform can bring new approaches to human resources. The platform helps organizations with the management of talent, skills assessment, and enacting contract agreements (www.bitcoinmagazine.com).

6. Conclusions

In Australia, the construction industry plays a great role in the national economy. Cartwright [31] states that the size of the Australian construction industry is 8% of the total gross domestic product (GDP), amounting to AUS$134 billion, which makes it the largest non-service industry in the country. As discussed above, the construction industry is overwhelmingly contract-based. The Australian construction industry employs 1.1 million people, and construction software help the industry to save AUS$25 billion through effective resources management and cost-cutting.[31] The Australian construction industry is heavily contract-based, therefore, it can benefit tremendously from blockchain technology, which is taking various industries by storm. The Australian construction industry is already saving billions by the effective use of software through cost-cutting. Similarly, it is well poised to exploit the as-yet undiscovered potential of blockchain technology, and create value for suppliers and buyers. The procurement process should be geared towards value creation, Walker et al.[5] argue that value includes quality of relationships, trust, ethics, and governance. Blockchain-based contract management platforms offer to develop and maintain good relationships, build trust, and ensure prompt contracting, accountability and governance, as authorized stakeholders are allowed to change data, and it offers great transparency, as blockchain-based platforms are tamper-proof.

References

[1] Santos, Jose Maria Delos (2017) Blockchain as Project Management Platform, https://project-management.com/blockchain-as-a-project-management-platform/?fbclid=IwAR2WVwd2SntF_LLiPMsAEn496gBxX5FiH4jZIfL_eBdg85cmt3V352vBQPY accessed on Feb 22, 2019

[2] Zwikael, Ofer (2016) Editorial for IJPM special issue on project benefit management. IJPM 34

[3] PMI (2004) A Guide to Project Management Body of Knowledge (PMBOK) 3rd ed. Project Management Institute, Inc. Pennsylvania

[4] Introduction to project management, Boston, Course Technologies

[5] Walker, D.H.T., and Rowlinson (2008) (EDs) Procurement Systems: A cross-Industry project management perspective, London: Taylor & Francis

[6] Kloppenborg, Timothy J (2009) Contemporary Project Management, Mason, Cengage Learning

[7] Harink, J. H. A., (1999) Excelling with E-procurement: The Electronic Highway to Competitive Advantage, Alphen aan Den Rijin, Holland, Samson, as cited in Thai, Khi V., (Ed) (2009) International Handbook of Public Procurement, CRC Press: London
[8] Walker D.H.T, and Hampson, Keith (2003) (Eds) Procurement Strategies: A Relationship-based Approach, Oxford: Blackwell Publishing
[9] Mohsini, R. and Davidson, C. H., (1989) as cited in Walker, D.H.T., and Rowlinson (2008) (EDs) Procurement Systems: A cross-Industry project management perspective, London: Taylor & Francis
[10] Lenard, D., and Mohsini, R (1998) as cited in Walker, D.H.T., and Rowlinson (2008) (EDs) Procurement Systems: A cross-Industry project management perspective, London: Taylor & Francis
[11] Masterman, J.W.E (1992) An Introduction to Building Procurement Systems, London: E& FN Spon
[12] Procurement Systems Manual (1994) NSW Public Works, https://www.procurepoint.nsw.gov.au/policy-and-reform/nsw-government-procurement-information accessed on Sept 9, 2014.
[13] Dalrymple, J., Boxer, L., and Stapples, W. (2006) as cited in Oyegoke S Adekunle, Dickinson Michael, Khalfan, Malik M.A., McDermott, Peter, Rowlinson, Steve (2009) "Construction project procurement routes: an in-depth critique", International Journal of Managing Project in Business, Vol. 2 No. 3
[14] Akintoye, Akintola (1994) "Design and build: a survey of construction contractors' views", Construction Management and Economics, 12
[15] Raisbeck, Peter, Duffield, Colin and Xu, Ming (2010) "Comparative performance of PPPs and traditional procurement in Australia", Construction Management and Economics, Issue 28
[16] Walker, C and Smith, A. J. (1995) as cited in Walker D.H.T, and Hampson, Keith (2003) (Eds) Procurement Strategies: A Relationship-based Approach, Oxford: Blackwell Publishing
[17] Buljevich, E.C. and Park , Y. S (1999) as cited in Oyegoke S Adekunle, Dickinson Michael, Khalfan Malik M.A., McDermott Peter, Rowlinson Steve (2009) "Construction project procurement routes: an in-depth critique", International Journal of Managing Project in Business, Vol. 2 No. 3
[18] Chen, Chuan, and Doloi, Hemanta (2007) "BOT application in China: Driving and impeding factors" International Journal of Project Management, 26

[19] Hwang Bon-Gang, Zhao Xianbo, and Gay, Mindy Jiang Shu (2013) "Public private partnership projects in Singapore: Factors, critical risks and preferred risk allocation from the perspective of contractors
[20] Chowdhary, A. N., Chen, P. H., and Tiong, R. L. K., (2011) as cited in Hwang Bon-Gang, Zhao Xianbo, and Gay, Mindy Jiang Shu (2013) " Public private partnership projects in Singapore: Factors, critical risks and preferred risk allocation from the perspective of contractors
[21] Cambridge Economic Policy Associates (2005) as cited in Raisbeck, Peter, Duffield, Colin and Xu, Ming (2010) "Comparative performance of PPPs and traditional procurement in Australia", Construction Management and Economics, Issue 28
[22] Kakabadse, Nada K., Kakabadse, Andrew P., and Summers, Nick (2007) Effectiveness of private finance initiatives (PFI): study of private financing for the provision of capital assets for schools, Public Administration and Development, Vol 27 (1)
[23] Mosey, David (2009) Early Contractor Involvement in Building Procurement: Contracts, Partnering and Project Management, UK: Wiley-Blackwell
[24] Francis, V. E and Sidwell, A.C (1996) as cited in Walker, D.H.T., and Rowlinson (2008) (EDs) Procurement Systems: A cross-Industry project management perspective, Taylor & Francis: London
[25] Sidwell, A. C and Ireland, V (1989) as cited in Walker, D.H.T., and Rowlinson (2008) (EDs) Procurement Systems: A cross-Industry project management perspective, London: Taylor & Francis
[26] Love P. E. D, Irani, Z., Cheng, E., and Li, H (2002) "A model for supporting inter – organizational relations in the supply chain", Engineering, Construction and Architectural Management, Vol. 9 No. 1, as cited in Oyegoke S Adekunle, Dickinson Michael, Khalfan Malik M.A., McDermott Peter, Rowlinson Steve (2009) "Construction project procurement routes: an in-depth critique", International Journal of Managing Project in Business, Vol. 2 No. 3
[27] Bennett, J (1986) as cited in Love, P.E.D, Skitmore, M., and Earl, G., (2010) "Selecting a suitable procurement methods for a building project", Construction Management and Economics 16:2.
[28] Robert, Johnston (2004) as cited in Walker, D.H.T., and Rowlinson (2008) (EDs) Procurement Systems: A cross-Industry project management perspective, London: Taylor & Francis
[29] Raymond, Jeanette (2008) "Benchmarking in public procurement", Benchmarking: An International Journal, Vol. 15 No.6
[30] Medina, Edgar (2018) How Blockchain going to change project management,

https://blog.workep.com/how-is-blockchain-going-to-change-project-management?fbclid=IwAR1-VCATcNxS4DMTPdw-HORNHadAJmZIbzZZbUMoI5DeKGTW_XQNFqB1nBE, accessed on Feb 22, 2019.

[31] Cartwright, David (2018) 10 Statistics Defining Australian Construction Industry https://www.buildsoft.com.au/blog/10-statistics-defining-the-australian-construction-industry, accessed on Feb 22, 2019

[32] BITCOIN Magazine (2019) Blockchain-Based Architecture For Project Management, https://bitcoinmagazine.com/articles/alehubs-new-blockchain-based-architecture-project-manageme/?fbclid=IwAR2ObFRhB3iwFZ6AT97oGIO5KRbibJU5t8RXzGm9oXh4rBlI_uayWswaOak, accessed on Feb 22, 2019

[33] PMPeople (2018) Blockchain to implement Trust in Project Management, https://medium.com/@pmpeople/blockchain-to-implement-trust-in-project-management-64e63f2a797d?fbclid=IwAR0aGOGVtWWtnGHpH1hHia_INjLR2IfOzeR68z0FUW6emytYBsoU7hSPrtc , accessed on Feb 22, 2019

Authors Biography

Tahmina Rashid is an Associate Professor of International Studies, Faculty of Arts & Design, University of Canberra Australia. Previously she served as Associate Dean for Academic Affairs at College of Arts & Sciences, Qatar University; Program Director International Development, RMIT University, Australia; and as Assistant Professor, Political Science in Pakistan. Her previous work includes "Contested Representations: Punjabi Women in Feminist Debates in Pakistan" and "International Development: Linking Academia with Development Aid & Effectiveness". She is a development consultant and has worked with UNWomen, UNESCO, GRM and Scopeglobal.

Munir Ahmad Saeed is currently enrolled in Professional Doctorate of Project Management at University of NSW, Australia. His research is focused on investigating Project Benefits Realization practices. He is working as Lecturer at College of Business, Canberra Institute of Technology, Canberra, Australia. Saeed has worked as a journalist in Pakistan for 10 years and has abiding interest in politics and current affairs. Saeed holds Bachelor of Arts, Bachelor of Business, Master of

English Literature and Master of Project Management (with Distinction) from Pakistani and Australian universities.

Mohiuddin Ahmed attained his PhD in Computer Science from UNSW Australia. His research expertise encompasses cyber security and machine learning, and covers a wide range of application domains. Mohiuddin holds over five years of data science and cyber security experience. He is currently working as a Lecturer in Computing and Security Sciences in the School of Science at Edith Cowan University. Prior to joining ECU, he served as a Lecturer in the Centre for Cyber Security and Games at Canberra Institute of Technology (CIT) and was also involved with CIT's Data Strategy Working Group.

CHAPTER SIX

BLOCKCHAIN TECHNOLOGY FOR PROTECTING PERSONAL INFORMATION PRIVACY

JINHONG YANG[1], MD MEHEDI HASSAN[2] AND CHUL-SOO KIM[2]

[1]Department of Healthcare and IT, Inje University, Korea
[2]Department of Computer Engineering, Inje University, Korea

Abstract

A large amount of personal information is being collected by enterprises for data-driven market investigation and forecasting. However, enterprises are often failing to preserve the privacy and security of collected personal data. Therefore, identifying a 'trust by design' data management tool, which balances data analysis and privacy protection, has become necessary. Recently-evolved blockchain technology which is decentralized and tamper-proof in nature, successfully addresses the privacy issues of personal information management. This chapter offers a summary of blockchain technology, personal information, and associated data privacy regulations. The chapter demonstrates a few blockchain schemes for personal information gathering, tracking, and sharing. It also advocates blockchain conflicts with Section 1 and Section 4 of the general data protection regulation (GDPR). A couple of methods for adopting privacy regulations by blockchain technology are well-elaborated, with explanations. This chapter identifies that to comply with the GDPR, separate storing of personal and non-personal information is needed. Alternatively, a block data modifiable blockchain architecture is needed. Similarly, actions to be taken by blockchain entrepreneurs and privacy policymakers are well acknowledged by this chapter. This chapter proposes two schemes for secure distribution of personal information. The first scheme proposes data access tracking with the help of blockchain as a service (BaaS). In the second scheme, BaaS technology tracks regular

updates of privacy terms to increase personal information privacy. Finally, instead of cryptocurrency and distributed service apps, blockchain technology will move in the cloud (as a service) for privacy managing and information tracking.

Keywords: Blockchain; personal data management; distributed ledger technology; personal information; data privacy; data security; blockchain issue; privacy; blockchain as a service; BaaS, bitcoin.

1. Introduction

Third-party data collection techniques leak huge amounts of personal data through malpractice, identity theft, spamming, and phishing. [1] Data has become ‘a new oil’, and ‘a weapon’, of modern warfare. Similarly, the lack of balance between personal data usage and privacy protection is frequently noticed. To resolve this issue, a data management platform using a ‘trust by design’ concept can generate privacy-preserved personal data supervision. The fourth industrial revolution [2] will expose a higher amount of personal data in comparison to the last three industrial revolutions. Recent information leaking practices [1] [3] [4] [5] are mostly caused by inefficient data management and storing platforms. [6] [7] Omer [8] identified three main factors in personal information privacy leaking: a) lack of standardization in cloud storage; b) collection of more information than is actually required; and c) distribution of excessive data for analytics. Several international institutions [9] [10] have also introduced guidelines to reduce personal information loss. Recently, Juniper stated that the yearly financial loss caused by information breaching would be around 2.1 trillion US dollars by the end of 2019. [11] However, regulation frequently reduces data analyzing scope, which also affects the quality of user experience.

On the contrary, ‘immutable’ decentralized technology — ‘blockchain’ — is becoming popular for reliable data management. Bitcoin was the first use-case of blockchain technology. [12] Scalability, transparency, decentralization, and secured communication, are the top four blockchain technology features that can mobilize information security for upcoming industrial revolutions. [13] [14] Blockchain offers trusted infrastructure that can manage user identity in a decentralized way. Blockchain technology successfully addresses key personal data risks by providing data gathering, sharing, managing, and tracking platforms. [15] As personal data is not only about security, but also privacy, existing

blockchain architecture is facing a huge obstacle to adopting existing data privacy regulations. [16] Recently introduced general data protection regulation (GDPR) includes the 'right to be forgotten, and 'should be erasable', data subject rights. Alternatively, the architecture of blockchain technology does not allow easy deletion of stored information. Therefore, conflict has already started between blockchain technology and privacy regulations. This chapter critically analyzes existing blockchain use-cases from the privacy and security aspects. This chapter analyzes key challenges and issues of blockchain technology in personal data management, to contribute the following:

- An introduction to the properties and working mechanism of blockchain technology,
- A presentation of personal information overview,
- Recognition of existing personal information regulations and standardization issues,
- Identification of the use of blockchain technology in personal data management,
- Mention of use-cases of blockchain technology in personal data management,
- Proposal of a few novel privacy-preserving schemes,
- Critical analysis of privacy regulations conflict with blockchain technology.

2. Blockchain Technology

The blockchain is a decentralized distributed ledger technology. Two versions of this technology were mentioned in a study by Swan (2015). [17] Blockchain technology is being used both in cryptocurrencies (version 1), and beyond cryptocurrencies (version 2). Decentralization, persistency, anonymity, and auditability, are four key features of blockchain. [18] The market for blockchain from 2018 to 2023 is predicted to expand at a compound annual growth rate (CAGR) of 80.2%, with global market size of USD 7683.7 by 2022. [19] The first use of this technology was a cryptocurrency (bitcoin). [12] This technology is also used by other industries like education,[20] human resource management, [21] the internet of things, [22] healthcare and medical, [23] vehicle sharing, [24] etc. In addition, blockchain technology is also in use for personal data management, sharing, and tracking. [25] [26] PwC's global fintech report predicted that around 77% of respondents want blockchain in some part of their industrial production system. [27] One of the key

drawbacks of blockchain technology is too much energy consumption by computer and network equipment. [28] Key blockchain components are discussed in Table I.

Table I: Components of Blockchain Technolgy

Blockchain terminology	Detailed descriptions
Block	A block consists of header, transaction counter and transaction. A block stores a transaction in an immutable way.
Block header	A block header contains the basic information of a transaction; as block version, timestamp, block verification difficulty, nonce, etc.
Transaction counter	It counts the serial number of a specific transaction.
Transaction data	This section varies based on blockchain usability.
Hash algorithm	The hash algorithm converts a specific length of input to a random value. Blockchain uses this to improve the security of transaction data.
Forking	As diverse participants must agree on a fixed rule, more than one chain may be generated. This manifold correct blockchain is forking.
Blockchain type	Blockchain technology is divided into three types based on its user-level permission: public, private, and consortium.
Consensus algorithm	A process by which a new block (transaction) is approved by a set of legal peers (blockchain node) is a consensus algorithm.

2.1 How Blockchain Works

The basic infrastructure needed for a blockchain platform is: nodes (participating entities), a set efficient computer system (interface for interaction), and a consensus algorithm (decision gathering procedure). A step-by-step blockchain transaction is stated here:

- Blockchain peers decide on transaction or exchange of information among themselves;
- All participated nodes approve the legitimacy of the initiated transaction;

- After a successful consensus, the new block is finalized;
- Detailed transaction information is included in a newly created block.

3. Personal Information and Identity Management

In this data-driven digital world, user-centric information is one of the vibrant forces to mobilize the digital economy. In this section, personal information types and associated privacy protection rules are elaborated.

3.1 Personal Information

Personal data or information is also known as either personally identifiable information (PII) or sensitive personal information (SPI) around the world. [29] Personal information can be in any form of digital data or opinion, about a precise individual whose identity can be revealed from that data. Personal information can be direct or indirect. Direct identifiers can identify a person. Direct identifiers are known as personally identifiable information (PII). Pfitzmann [30] defined personally identifiable information as follows:

> "An identity is any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons."

The National Technical Information Service (NTIS) [31] defined personally identifiable information as:

> "Any information about an individual maintained by an agency, including (PII) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (linked PII) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

Another concept of personal information is indirect identifiers (quasi-identifiers) or potential personally identifiable information (PPII). Pfitzmann [30] introduces this information as follows:

> "A partial identity is a subset of attribute values of a complete identity, where a complete identity is the union of all attribute values of all identities of this person."

Table II: Personally Identifiable Information (PII) and Potential Personally Identifiable Information (PPII) [16-18]

Personally identifiable information (PII)	Potential personally identifiable information (PPII)
Birth date, full name, telephone number, security number, tax identification info, credit card information, location, driving license information, patient identification detail, vehicle registration number, credit card, etc.	Birthdate, partial name, job detail, IP address, race, blood group, website cookie, education, educational status, car name, sports preference, political view, living area, social network info, age, etc.

3.2 Personal Information Regulations

3.2.1 General Data Protection Regulation (GDPR)

GDPR [32] has applied to organizations across the world since 25 May 2018. As GDPR is a regulation, not a directive, new legislation was not needed, instead, it became applicable automatically. No endorsement from parliament or international organization is needed in GDPR execution. Punit [33] mentioned the ten key GDPR requirements as: lawful, fair and transparent processing; data protection officer employment; awareness and training; data transfer; privacy by design; user consent; data subject rights; data protection and impact assessment; limitation of purpose; and data and storage. GDPR introduces three data handlers: data user, controller, and processor. The data user produces information, the controller collects the data for service giving, and the controller uses a processor for data analysis. [10] GDPR regulates the location of personal data processing. Processing, storing, and analyzing personal information of the European Union (EU) must occur within European territory. In contrast, it demands the 'right to forget' user information, or that it should be 'erasable' (Article 42 and Article 25). [32] This means both the controller and the processor are bound to delete users' personal information on demand. People can demand data erasure, verbally, or in writing. According to GDPR, the controller and the processor have one month to respond to a data delete request. [10]

3.2.2 Health Insurance Portability and Accountability Act (HIPAA)

In 1996, the department of health and human services of the United States (US) introduced the data privacy and security act for safeguarding medical information. The HIPAA [9] has two main purposes: easing health insurance coverage, and reducing the administrative burden during electronic data sharing. [34] The HIPAA introduced two methods to protect personal information:

- Safe harbor: Safe harbor relies on the elimination or simplification of 18 sensitive data elements from the user data (e.g. name, phone number, email address, patient identity, etc.).
- Expert determination: The expert determination method uses expert opinion, knowledge, and experience, with generally accepted scientific principles. Experienced people use detailed observation methods to remove individually identifiable information from the user data. Expert determination is used less frequently than safe harbor.

3.2.3 Privacy law in Australia

Data privacy in Australia is protected by several territorial acts. [35] The Privacy and Personal Information Protection Act (PPIPA) of 1998 regulates information privacy in New South Wales (NSW). However, PPIPA only applied to the public sector, not health privacy. In Victoria, personal data privacy is managed by the Privacy and Data Protection Act of 2014. In Queensland, The Information Privacy Act of 2009 regulates personal data privacy issues. The Information Privacy Act regulates the collection and handling of personal information of Canberra state.

3.2.4 Personal Information Protection Act South Korea

The purpose of this Act is to protect the personal data of South Korean citizens from unnecessary gathering, unauthorized use or exposure, and misuse, [36] although data breaching notification is out of the scope of the Act.

4. Blockchain Technology for Identity Management

Several technologies are already capitalizing on blockchain for privacy-preserved data management. Within the last couple of years, blockchain has become one of the mainstream technologies for secure identity

management. Companies are leveraging blockchain technology in several phases of data management. At the moment, we can see how blockchain technology can serve trust-based data management during personal data handling.

4.1 Personal Data Collection

Companies collect personal information while initiating services for the user. During this data collection, consent from several involved parties is often required. Blockchain technology can minimize the cost of overall consent gathering with the distributed network. With this consensus from all parties, blockchain can specifically inform a selected company or blockchain node of this data collection. Blockchain can hide a specific data collection from an unwanted third party. Finally, blockchain can provide, minimize, inform, control, aggregate, and hide services to a personal data handling company.

4.2 Personal Data Storage

After data is collected, the organization faces real difficulty during data storing and managing. Secured blockchain technology can store data in a decentralized way. Decentralized data storing assures separate data gathering in multiple physical locations. Blockchain technology improves the overall security of the collected information. Transparency of any personal data is strongly preserved by blockchain. Aggregated decisioning during data storage among multiple data storing entities ensures better security of personal data. Blockchain preserves the control of the data only to the specific data owner.

4.3 Personal Data Usage

Once personal data has moved from user to controller, usage of that sensitive personal information should be monitored closely. Blockchain technology can store data usability scope in an immutable blockchain database. Later, users and companies can follow that usability scope during the use of specific personal information. Blockchain technology can inform and control the usage of personal data.

4.4 Personal Data Sharing

Sharing of personal information is another highly sensitive phase of the personal data life cycle. To gain financial profit from personal data, companies frequently share that personal data with other data analyzing companies. Blockchain technology can provide a controlling service during data sharing. Blockchain can store the identities of data exchanging companies.

4.5 Personal Data Destruction

Blockchain can also be used in personal data destruction after successful use. Private and consortium blockchains can gather consensus from involved companies and delete personal data, although permanent deletion of personal information from public blockchain is in doubt. Blockchain can check the available hash value of a specific block to ensure complete erasure of personal data.

4.6 Personal Data Breach Penalty

As blockchain can track data usability scope, identifying a corrupted node has become much easier. Blockchain technology can track data collection, data storage, data sharing, and data destruction. Therefore, data manipulation is trackable with blockchain services. Blockchain ensures accurate penalties for any data stakeholders (user, controller, or processor) for data breaching incidents.

5. Use of Blockchain Technology for Personal Data Management

The last section discussed how blockchain technology can be utilized in several phases of personal data handling. Here, we discuss a few uses of blockchain technology.

Guy Zyskind [26] proposed an off-the-chain blockchain architecture. The study decentralized personal data privacy with distributed blockchain technology. Zyskind mentioned three entities users, services, and nodes. The study implemented a platform that enables personal data sharing among those entities. The study introduced an off-the-chain blockchain technology that stored sensitive personal information in a local database. This way of personal information storing enables easy deletion of personal

information from a public blockchain. The study satisfies Articles 17 and 4 of the GDPR [10] by including this personal data delete feature in blockchain technology. It implements a protocol that changes a distributed ledger into an automated access-control administrator that does not need trust in data sharing entities, although, this off-chain data may not preserve the same security feature of the on-chain blockchain. The study could not fully secure 'off-the-chain' blockchain data. Since off-chain data is easily accessible, local database copy can leak sensitive personal information.

Blockchain-based transparent storing and distributing of IoT information was proposed by Hossein. [37] The study introduced 'data place' and 'control place' into the IoT environment. The control plane consists of virtual chain and blockchain. The data plane is formed with the routing layer and the storage layer. The study maintained three basic characteristics and designed a privacy-aware blockchain architecture. Firstly, the system was (R1) decentralized and resilient in nature; secondly, the system secures the confidentiality of the data storage; and finally, the system was IoT compatible. However, the lack of an energy-efficient IoT sensor questioned this method. [38]

Blockchain allows organization of personal information processing in the IoT ecosystem, which was proposed by another study [39]. This study proposes ADVOCATE, a framework which enables processing of personal information which is compliant with GDPR terminologies. A notary service was also introduced by this study. The main goal of that service was to ensure user security consents. Moreover, the notary service could provide an intelligent assessment of user consents.

Personal identity management and associated data security were studied by Shrier. [40] The study pointed out that new blockchain architecture is needed for introducing blockchain on a large scale. The study demands three levels of architectural change in blockchain technology. Firstly, the system must allow available nodes to verify the identity of all other blockchain nodes. Secondly, blockchain identity independence should be well measured. Finally, the source of any digitally gathered identity must be well assessed by the blockchain system. The report also mentioned another architecture, named ChainAnchor. ChainAnchor is an architecture over blockchain technology that ensures the identity of the permissioned blockchain. An unidentified identity authentication procedure allows anybody to read and authenticate blockchain transactions. However, only anonymous verified identities from a particular blockchain can process the transactions.

Personally identifiable information linking with providers before sharing was proposed by Banerjee. [41] The study combined data privacy ontology with blockchain technology to propose a tool. The tool automated access and control of the data collector, and tracked associated data distribution. Linkshare is implemented by those who store personal information and blockchain privacy policies in a tree-like structure.

Liang [42] proposed ProvChain architecture, which has three stages: data provenance, storing of provenance information, and associated validation. This study introduced the user, cloud service providers, provenance auditors, and the blockchain network. The architecture first collects data in cloud storage and publishes the collected information to the blockchain network (cloud) for verifying the nodes and data. Finally, after a successful consensus, provenance databases are updated accordingly.

Karuna [43] proposes compliance privacy concerning regulation by automating privacy policy with blockchain technology. This study firstly identifies key elements of personal data policy documents. With semantic web technology, this study translates paper regulations into some graph-based rules. Secondly, the study recognizes key data handling operators. Finally, the proposed study saturates privacy-preserved information only before adding to the blockchain.

Personal data includes healthcare data. Laure [44] mentioned that interoperability issues among several blockchain technologies might degrade extensive use of blockchain technology in the healthcare industry. The study encouraged health blockchain systems developers to empower users in order to increase data privacy. The need for basic access control permission was proposed by this study. Accessing of a sensitive block must be regulated based on patient permission. The study proposed a ‘healthcare data lake’ to increase scalability, access security, and information privacy, of the overall system.

To have control over every piece of social media content, Chakravorty [45] proposed ‘Ushare’, which is a permissioned blockchain. Personal information shared in social media is encrypted with a personal certification authority (PCA). The functionalities of ‘Ushare’ are maintained as separate sub-functions. Firstly, blockchain tracks all data owners. Secondly, blockchain counts the number of allowed shares for particular data. Thirdly, the system keeps track of two-level keys (public-private keys) for every piece of content. Finally, a user has full control

over his/her personal information encryption methodologies and associated contents.

The rapid growth of the internet of things (IoT) devices brings more risk to our personal information. IoT devices handle enormous personal information among IoT devices and associated servers. Due to decentralized topology and resource restrictions, personal information security and privacy are at stake. Dorri[46] proposed an energy efficient blockchain technology for IoT while maintaining the security features of the blockchain. The proposed architecture uses overlay network and cloud storage with blockchain technology to secure personal information that IoT devices exchange among themselves.

Burst IQ [47] offers a blockchain-based healthcare data exchanging platform. It offers an individual life graph with user data, and stores it in a health wallet. Afterwards, that wallet can share, manage, sell, and donate individual information, according to user decision. This is also HIPAA, GDPR and NIST compliant, and also supports a larger volume of health data.

MedRec by Azaria [48] provides a complete platform for patient data authentication and sharing among stakeholders. This blockchain system introduced incentives for successful data sharing and verification. This keeps a data sharing log for transparent auditability.

Jonas, [49] Blinking, [50] and Nasr, [25] proposed a few GDPR-compliant blockchain architectures for data sharing and tracking. These studies demonstrated the involvement of GDPR components (user, controller, and processor) with blockchain architecture (nodes, consensus, local database). Although the proposed techniques reduce basic blockchain security facilities, they increase key personal data privacy. [51]

Yang [52] introduced a collaboration-based medical decision-making blockchain scheme, along with a consensus algorithm proof of familiarity (PoF). The study stores and distributes critical medical decisions for treatment where a specific domain experience of key decision makers was considered.

6. Challenges, Issues and Solutions

In the last few sections we discussed how blockchain is being used for personal data handling. In this particular section, we will discuss a few challenges and issues of blockchain technology.

6.1 Blockchain Technology vs Data Privacy Law

As an emerging technology, blockchain is still facing data privacy regulations. We will now mention a few significant aspects of blockchain's adaptation to privacy terms. [53] In this chapter, we will mainly focus on the general data protection regulation (GDPR) act imposed by the European Union on 25 May 2018.

6.1.1 Accountability in a Blockchain?

According to GDPR (section 4), [54] a single person or a company should be solely responsible for the handling of personal data. However, under decentralized blockchain architecture, it is always difficult to identify the actual owner of personal data. Nevertheless, a specific controller or processor must be identified in case of any data breaching incident. Thus, GDPR and blockchain technology conflict with a centralized and decentralized architecture.

6.1.2 The Lawfulness of Data Processing

According to GDPR (section 6), [54] data gathering and processing consent must follow data privacy rules. However, during a blockchain consent gathering, there is not much scope for data privacy law checking. Moreover, the data processor cannot gather and process personal information forever. According to GDPR, the controller and the processor must delete personal information after necessary use (unless any legal obligation is there). Contrarily, blockchain stores data permanently.

6.1.3 The Obligation to Inform and Rights of the Data Subject

According to GDPR (sections 13,14 and 15), data subjects' rights must be respected. At the same time, the responsible controller and processor must inform the data owner about any data sharing incident. Private blockchain [55] might share data among controllers and processors without any user acknowledgment.

6.1.4 Blockchain Technology and the 'Right to Be Forgotten'

First of all, GDPR (section 1, article 4) and other privacy regulations apply only on personal data. However, blockchain technology does not handle direct personal information like name, address, email, etc. Alternatively, blockchain stores hashes, and public and private keys. From this viewpoint, blockchain and GDPR do not have a legal conflict. However, based on usability and access control of public-private key blockchain may not be completely anonymous. [25] [44] Again, article 17 of the GDPR [32] strictly maintains the 'right to be forgotten' and 'right to erasure'. Blockchain faces two possible scenarios in this situation: [56] [57]

- Permissioned or private blockchain: Consensus from available blockchain nodes can lawfully delete any blockchain node. However, participants must cooperate with each other in a trusted environment.
- Public or permissionless blockchain: Oppositely, removal of personal information from open blockchain platforms [58] which are cryptocurrencies, is almost impossible.

Data erasure and editing are in direct conflict with blockchain. On fundamental points, blockchain fully opposes the GDPR mandates. It relies on a distributed ledger system that is intended to be a permanent and rigid record-keeping storage. Therefore, the question remains open, which will change itself to accommodate others – blockchain, or GDPR?

6.2 Blockchain Technology and the Internet of Things (IoT)

Several blockchain technologies have already developed without the real implementation of the whole system. [59] Therefore, IoT issues like energy consumption, lack of accessibility, lack of standardization and device compliance were overlooked. As the IoT collects huge amounts of personal information, blockchain must handle those, considering the architectural drawbacks of IoT sensors. [60] Moreover, blockchain technology is equipped with highly secured encryption mechanisms. Oppositely, IoT infrastructures are comparatively light and less secure. [61] Therefore, blockchain implementation in the IoT needs large scale design modification of blockchain technology. [62]

6.3 Possible Solutions for Personal Information Sharing and Tracking

As blockchain implementation, management, and maintaining, are costly, blockchain as a service platform is becoming popular. Blockchain as a service (BaaS) means building, managing, hosting, and using, various aspects of blockchain technologies, such as applications, nodes, smart contracts, and distributed ledger, on the cloud. Such cloud-based services facilitate block-chain set-up, platform, security, and other associated features. Thus, BaaS introduces the blockchain service platform, supporting blockchain core features, based on cloud computing infrastructure with the integrated developing environment, for both the developers and the consumers. [63] Based on this rising BaaS platform, this chapter proposes two possible personal information privacy preserving blockchain solutions, as follows.

6.3.1 Data Specific Access Tracking with Blockchain as a Service (BaaS) platform:

Cloud storage should store sensitive personal information like photos, emails, signatures, contact information, location data, etc. Upon using (accessing) that information, a new block will be generated which will store associated data accessing information (Figure 1). Companies like A, B, C and N can access personal information, like location, photos, emails, and N, stored in the cloud. While doing so, transactions are stored in a separate block, like block 0, block 1, block 2 and block N. So, in future, an individual can use tracking in any breaching case.

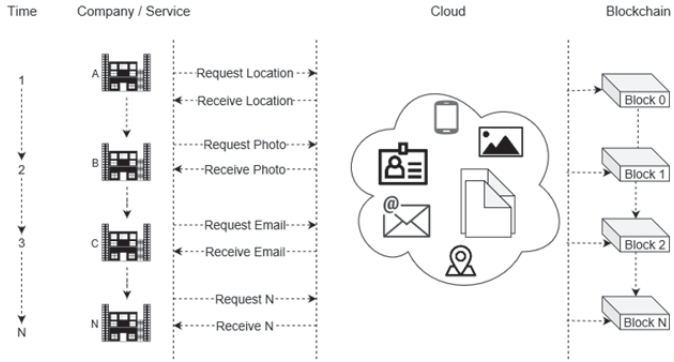


Figure 1. Data specific access tracking with blockchain as a service (BaaS) platform

6.3.2 User Data Privacy Terms Monitoring with Blockchain as a Service (BaaS) Platform:

The user frequently provides personal information in different ranges, while registering and login to web services. The user also agrees with privacy terms and data usability. However, companies frequently update and change privacy terms and data usage from time to time. Unfortunately, the user cannot monitor service privacy terms changes to control the usage of his/her sensitive personal information. This chapter proposes blockchain (BaaS) as a service platform assistant data privacy terms tracking scheme (Figure 2). A user uses personal information (phone number, email, photo id) to register for Service A. At the same time, the user also agrees to the privacy terms. The user can login again, with Google ID, at time 3. If all three incidents are recorded in block 0, block 1 and block 2, in the case of privacy terms changes, at login time 4, the user can track the changes. Finally, the associated changes are stored at Block N.

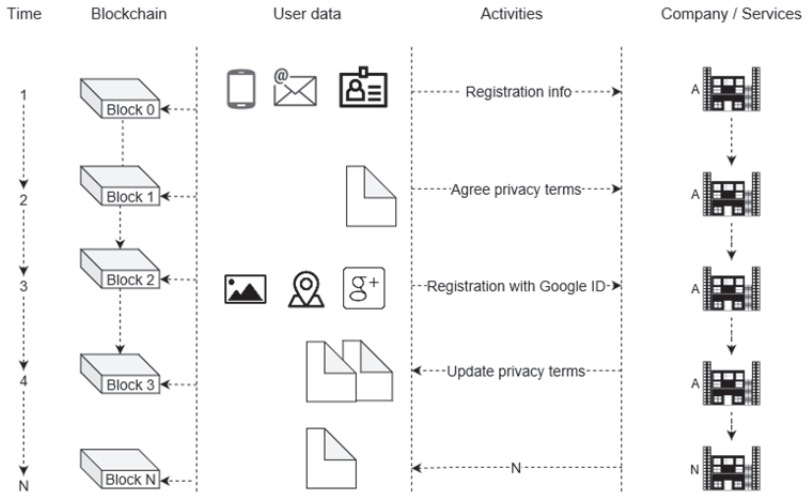


Figure 2. User data and privacy terms tracking with blockchain as a service (BaaS) platform.

7. Conclusion

The privacy of personal information can be endangered by several means. [64] As blockchain technology (distributed ledger) has already gained

enough trust to prove it to be a 'trusted machine', [65] [66] therefore the use of blockchain technology in various sectors is increasing too. This chapter shows several use cases of blockchain technology, where the use of personal information was noteworthy. Due to blockchain's decentralization and tamper-proof features, this technology is being used in healthcare, the IoT, finance, smart industry, etc. Moreover, the chapter identifies how personal information is leaked. Similarly, a number of data protection regulations were also discussed in this chapter. This chapter explains key blockchain features and the working procedure of blockchain technology. Finally, the chapter also includes two blockchain schemes for increasing personal data privacy with the help of blockchain technology.

Irrespective of the aforementioned advantages of blockchain technology, personal data privacy regulations are frequently conflicting with it. Blockchain technology is unable to protect several key aspects of GDPR. Use of private and public blockchain should be standardized at corporate level to secure the sustainable future of blockchain technology. This chapter explains a few privacy-preserved blockchain architectures for personal data management. Privacy by blockchain design is necessary for adopting blockchain technology in upcoming privacy challenges. Scalability issues of blockchain technology must be overcome before it becomes part of mainstream technology. Laws, regulations, governance, and cooperation must adapt the blockchain technology, with a view to preserving privacy.

References

[1] "The Biggest Ever Data Breaches | Security | Techworld," 2019. [Online]. Available: https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/. [Accessed: 05-Mar-2019].
[2] K. Schwab, *The fourth industrial revolution*. Crown Business, 2017.
[3] "Guardian Top 10," 2018. [Online]. Available: https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time.
[4] N. Lord, "Top 10 Biggest Healthcare Data Breaches," 2018. [Online]. Available: https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time.
[5] C. S. Onik, M. M. H., Al-Zaben, N., Yang, J., Lee, N.Y., & Kim, "Risk Identification of Personally Identifiable Information from Collective Mobile App Data.," in *International Conference on Computing, Electronics & Communications Engineering 2018 (iCCECE '18)*, 2018,

pp. 71–76.
[6] "Top 5 Database Management Challenges - and How to Solve Them." [Online]. Available: https://micoresolutions.com/top-database-management-challenges/. [Accessed: 05-Mar-2019].
[7] M. M. H. ONIK, K. I. M. Chul-Soo, and Y. Jinhong, "Personal Data Privacy Challenges of the Fourth Industrial Revolution," in *2019 21st International Conference on Advanced Communication Technology (ICACT)*, 2019, pp. 635–638.
[8] O. Tene and J. Polonetsky, "Big data for all: Privacy and user control in the age of analytics," *Nw. J. Tech. Intell. Prop.*, vol. 11, p. xxvii, 2012.
[9] "HIPAA (Office for Civil Rights)," 2018. [Online]. Available: https://www.hipaajournal.com/healthcare-data-breach-statistics/.
[10] D. R. G. MARTIN and S. PALLADINO, "What is GDPR, Why it is Needed & How to Prepare," 2017.
[11] "Cybercrime will Cost Businesses Over $2 Trillion by 2019." [Online]. Available: https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion. [Accessed: 05-Mar-2019].
[12] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[13] S. R. Chhetri, N. Rashid, S. Faezi, and M. A. Al Faruque, "Security trends and advances in manufacturing systems in the era of industry 4.0," in *Computer-Aided Design (ICCAD), 2017 IEEE/ACM International Conference on*, 2017, pp. 1039–1046.
[14] M. M. H. Onik and M. Ahmed, "Blockchain in the Era of Industry 4.0," in *Data Analytics: Concepts, Techniques, and Applications*, A.-S. K. P. Mohiuddin Ahmed, Ed. CRC Press, 2018, pp. 259–298.
[15] M. H. Miraz and M. Ali, "Applications of Blockchain Technology beyond Cryptocurrency," *Ann. Emerg. Technol. Comput.*, vol. 2, no. 1, pp. 1–6, Jan. 2018.
[16] A. P. Joshi, M. Han, and Y. Wang, "A survey on security and privacy issues of blockchain technology," *Math. Found. Comput.*, vol. 1, no. 2, pp. 121–147, 2018.
[17] M. Swan, *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.," 2015.
[18] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Big Data (BigData Congress), 2017 IEEE International Congress on*, 2017, pp. 557–564.
[19] "The Global Market for Blockchain (2018-2023): Projected to

Expand at a CAGR of 80.2% - ResearchAndMarkets.com | Business Wire," 2018. [Online]. Available: https://www.businesswire.com/news/home/20181210005600/en/Global-Market-Blockchain-2018-2023-Projected-Expand-CAGR. [Accessed: 26-Feb-2019].

[20] A. Islam, M. Kader, and S. Y. Shin, "BSSSQS: A Blockchain Based Smart and Secured Scheme for Question Sharing in the Smart Education System," *arXiv Prepr. arXiv1812.03917*, 2018.

[21] M. M. H. Onik, M. H. Miraz, and C.-S. Kim, "A Recruitment and Human Resource Management Technique using Blockchain Technology for Industry 4.0," in *Proceedings of the Smart Cities Symposium (SCS-2018)*, 2018, pp. 11–16.

[22] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, *Blockchain and iot integration: A systematic survey*, vol. 18, no. 8. 2018.

[23] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on*, 2016, pp. 1–3.

[24] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-VN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City.," *JIPS*, vol. 13, no. 1, pp. 184–195, 2017.

[25] N. Al-Zaben, M. M. H. Onik, J. Yang, N.-Y. Lee, and C.-S. Kim, "General Data Protection Regulation Complied Blockchain Architecture for Personally Identifiable Information Management," in *International Conference on Computing, Electronics & Communications Engineering 2018 (iCCECE '18)*, 2018, pp. 72–88.

[26] G. Zyskind and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," in *Security and Privacy Workshops (SPW), 2015 IEEE*, 2015, pp. 180–184.

[27] J. Plansky, T. O'Donnell, and K. Richards, "A strategist's Guide to Blockchain," *PwC Rep.*, 2016.

[28] M. M. H. Onik, N. Al-Zaben, H. Phan Hoo, and C.-S. Kim, "MUXER—A New Equipment for Energy Saving in Ethernet," *Technologies*, vol. 5, no. 4, p. 74, 2017.

[29] G. M. Stevens, "Data security breach notification laws." Congressional Research Service Washington, DC, 2012.

[30] A. Pfitzmann and M. Hansen, "Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology," *Version v0*, vol. 31, p. 15, 2008.

[31] E. McCallister, *Guide to protecting the confidentiality of personally identifiable information*. Diane Publishing, 2010.
[32] "GDPR-EU," 2016. [Online]. Available: https://gdpr-info.eu/art-4-gdpr/.
[33] Punit Bhatia, "GDPR summary: Overview of 10 key requirements." [Online]. Available: https://advisera.com/eugdpracademy/knowledgebase/a-summary-of-10-key-gdpr-requirements/. [Accessed: 01-Mar-2019].
[34] I. G. Cohen and M. M. Mello, "HIPAA and protecting health information in the 21st Century," *Jama*, vol. 320, no. 3, pp. 231–232, 2018.
[35] D. Watts and P. Casanovas, "Privacy and Data Protection in Australia: a Critical overview." W3C, 2018.
[36] "Personal Data Protection Laws in Korea." [Online]. Available: https://www.privacy.go.kr/eng/laws_policies_list.do. [Accessed: 01-Mar-2019].
[37] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of iot data," in *Proceedings of the 2017 on Cloud Computing Security Workshop*, 2017, pp. 45–50.
[38] N. Al-Zaben, M. M. H. Onik, C.-S. Kim, and J. Yang, "Communication Interface Identifier Protocol (CIIP): An Energy Efficient Protocol for smaller IoT Sensor," *arXiv Prepr. arXiv1902.02164*, 2019.
[39] K. Rantos, G. Drosatos, K. Demertzis, C. Ilioudis, and A. Papanikolaou, "Blockchain-based consents management for personal data processing in the IoT ecosystem," in *proceedings of the 15th International Conference on Security and Cryptography (SECRYPT 2018), part of ICETE*, 2018, pp. 572–577.
[40] D. Shrier, W. Wu, and A. Pentland, "Blockchain & infrastructure (identity, data security)," *Massachusetts Inst. Technol. Sci.*, vol. 1, no. 3, 2016.
[41] A. Banerjee and K. P. Joshi, "Link before you share: Managing privacy policies through blockchain," in *2017 IEEE International Conference on Big Data (Big Data)*, 2017, pp. 4438–4447.
[42] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, 2017, pp. 468–477.
[43] K. P. Joshi, A. Gupta, S. Mittal, C. Pearce, A. Joshi, and T. Finin,

"Semantic approach to automating management of big data privacy policies," in *Big Data (Big Data), 2016 IEEE International Conference on*, 2016, pp. 482–491.

[44] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*, 2016.

[45] A. Chakravorty and C. Rong, "Ushare: user controlled social media based on blockchain," in *Proceedings of the 11th international conference on ubiquitous information management and communication*, 2017, p. 99.

[46] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and solutions," *arXiv Prepr. arXiv1608.05187*, 2016.

[47] "Home New - burstIQ." [Online]. Available: https://www.burstiq.com/. [Accessed: 03-Mar-2019].

[48] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *Open and Big Data (OBD), International Conference on*, 2016, pp. 25–30.

[49] "Private data, a built-in 'GDPR compliant' solution for Hyperledger Fabric." [Online]. Available: https://hackernoon.com/private-data-a-built-in-gdpr-compliant-solution-for-hyperledger-fabric-5a35b91e6aaa. [Accessed: 03-Mar-2019].

[50] "Blockchain-based Digital ID solution." [Online]. Available: https://blinking.id/. [Accessed: 03-Mar-2019].

[51] M. M. H. Onik, C.-S. Kim, N.-Y. Lee, and J. Yang, "Privacy-aware blockchain for personal data sharing and tracking," *Open Comput. Sci.*, vol. 9, no. 1, pp. 80–91, 2019.

[52] J. Yang, M. Onik, N.-Y. Lee, M. Ahmed, and C.-S. Kim, "Proof-of-Familiarity: A Privacy-Preserved Blockchain Scheme for Collaborative Medical Decision-Making," *Appl. Sci.*, vol. 9, no. 7, p. 1370, 2019.

[53] "How do Blockchain and data privacy work together? | HÄRTING Rechtsanwälte," 2018. [Online]. Available: https://www.haerting.de/neuigkeit/how-do-blockchain-and-data-privacy-work-together. [Accessed: 03-Mar-2019].

[54] W. G. Voss, "European union data privacy law reform: General data protection regulation, privacy shield, and the right to delisting," 2017.

[55] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Futur. Gener. Comput. Syst.*, vol. 95, pp. 511–521, 2019.

[56] "Blockchain versus GDPR and who should adjust most." [Online]. Available: https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most. [Accessed: 03-Mar-2019].

[57] C. Wirth and M. Kolain, "Privacy by BlockChain Design: A BlockChain-enabled GDPR-compliant Approach for Handling Personal Data," in *Proceedings of 1st ERCIM Blockchain Workshop 2018*, 2018.

[58] M. H. Miraz and D. C. Donald, "Application of Blockchain in Booking and Registration Systems of Securities Exchanges," in *IEEE International Conference on Computing, Electronics & Communications Engineering 2018 (IEEE iCCECE '18)*, 2018, pp. 35–40.

[59] J. S. Park, T. Y. Youn, H. Bin Kim, K. H. Rhee, and S. U. Shin, "Smart contract-based review system for an IoT data marketplace," *Sensors (Switzerland)*, vol. 18, no. 10, pp. 1–16, 2018.

[60] A. Banafa, "IoT and Blockchain Convergence: Benefits and Challenges," *IEEE Internet Things*, 2017.

[61] B. Bostami, M. Ahmed, and S. Choudhury, "False Data Injection Attacks in Internet of Things," in *Performability in Internet of Things*, Springer, 2019, pp. 47–58.

[62] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet Things J.*, 2018.

[63] M. Samaniego, … R. D. I. of T. (iThings) and, and undefined 2016, "Blockchain as a Service for IoT," *ieeexplore.ieee.org*.

[64] M. M. H. Onik, N. Al-Zaben, J. Yang, and C.-S. Kim, "Privacy of Things (PoT): Personally Identifiable Information Monitoring System for Smart Homes," in *Proceedings of Symposium of the Korean Institute of communications and Information Sciences*, 2018, pp. 256–257.

[65] K. Siau and W. Wang, "Building Trust in Artificial Intelligence, Machine Learning, and Robotics," *Cut. Bus. Technol. J.*, vol. 31, no. 2, pp. 47–53, 2018.

[66] M. H. Miraz, "Blockchain: Technology Fundamentals of the Trust Machine," *Mach. Lawyering, Chinese Univ. Hong Kong, 23rd December*, 2017.

Authors Biography

Jinhong Yang received Ph.D. degree form Dept. of Information and Communications Engineering at KAIST, Korea in 2017. He was Chief Technology Officer (CTO) of HECAS Inc. and developed ultra-low latency mobile video streaming technology. In March 2018, he joined at Inje University, Gimhae, Korea as an Assistant professor. His research interests include CPS, IoT and Privacy technologies.

Md Mehedi Hassan obtained his B.S. from the Islamic University of Technology, Bangladesh. He is currently a master's candidate in the Dept. of Computer Engineering at Inje University, Korea. His research interests include data privacy, network security and blockchain technology. He is working to develop an efficient personal information protection and sharing platform to handle the emerging data privacy problems.

Chul-Soo Kim is a professor in the School of Computer Engineering of Inje University in Gimhae, Korea. He received Ph.D. from the Pusan National University (Pusan, Korea) and worked for ETRI (Electronics and Telecommunication Research Institute) from 1985 - 2000 as senior researcher for developing TDX exchange. Aside from the involvement in various national and international projects, his primary research interests include network protocols, traffic management, OAM issue, and NGN charging. He is a member of ITU-T SG3, SG11, SG13 and a Rapporteur of ATM Lite from 1998 - 2002, and CEO in WIZNET from 2000 - 2001. He is currently the chairperson of BcN Reference Model in Korea, and a Rapporteur of ITU-T SG3 NGN Charging

CHAPTER SEVEN

BLOCKCHAIN-ENABLED ENTREPRENEURIAL FINANCIAL FUNDING AND INVESTMENTS: THE NEW ERA OF INITIAL COIN OFFERINGS

DIMITRIOS SALAMPASIS, MARK PICKERING AND VOLKMAR KLAUßER

Department of Business Technology and Entrepreneurship, Swinburne Business School, Swinburne University of Technology, Australia

Abstract

Within the spectrum of research on fundraising mechanisms and activities for projects or new ventures, the term 'entrepreneurial finance' has emerged, looking into traditional and non-traditional ways for raising funds that are necessary for development, growth, and scale. Currently, the entrepreneurial financial funding and investments landscape is changing, due to the emergence of breakthrough technologies, aiming at fostering disruptive innovation, decentralization, and democratization of fundraising. Distributed ledger technology, and more specifically blockchain and Ethereum, are changing the way stakeholders invest, mainly through new mechanisms, one of which is the initial coin offering (ICO), a way of financing a cryptocurrency startup, or a startup company, by means of crypto-coins, providing resources to projects that otherwise might not go forward. This research aims at illuminating the invisible side of blockchain-enabled entrepreneurial finance, by providing an informative and comprehensive mapping of the ICO landscape in terms of understanding the trends, the process, the environment, and the applicability and challenges of this new capital-raising mechanism, while at the same time providing recommendations for future academic research, industry, policy-making, and regulation. This research is based on a

review of recent publicly-available information, along with, academic and industry literature.

Keywords: Entrepreneurial finance; initial coin offering; blockchain; crowdfunding; financial regulation; initial exchange offering; initial public offering; ICOs process; tokens; investment; cryptocurrencies.

1. Introduction

Initial coin offerings (hereinafter ICOs) have emerged and flourished as a niche form of private and decentralized fundraising for blockchain-related businesses. Companies raised a phenomenal US$10 billion globally during 2017, which grew to US$11.4 billion in 2018. [1] However, ICO levels have subsequently fallen in recent months. Latest figures for the period January 1 2019 - April 30 2019 show that 93 ICO projects were funded with companies, raising approx. US$855 million[1] cryptocurrency-based funding globally,[2] well below the value of the equivalent period of 2018. ICOs enable businesses to sell tokens (equity/asset tokens and utility/access tokens) or coins directly to the public over the internet. ICOs have significant benefits over traditional entrepreneurial sources of finance, such as founder bootstrapping, bank debt, angel investors, and venture capital, and initial public offerings (IPOs) for more advanced firms.

ICOs enable firms to raise substantial funds quickly, and cost-effectively, at a very early stage of their lives, facilitating rapid technology and business model development without giving up equity or taking on debt. Many of the blockchain models are network-related; the attractiveness of the business model for potential investors, and those targeted to use blockchain solutions, is impacted by having a critical mass of participants, particularly key industry players on the platform. [2] Presales, or airdrops of tokens or coins, are often made to key players, with the intent of incentivizing them to join the platform, and encouraging others to do so, with the potential of a substantial increase in the value of tokens during and after the ICO. [2] The ability to raise funds quickly to develop and market the blockchain platform may provide a first-mover advantage, and a barrier against future competing offerings.

While ICOs are an innovative, fast, and cost-effective way for blockchain-related businesses to raise entrepreneurial finance, it is important to consider the perspective of the investors from whom these billions of

dollars have been raised. ICOs provide a relatively unique vehicle for the public to participate in very early stage investments in a liquid form, with many, but not all of the coins issued being tradable on cryptocurrency exchanges. It has been argued, that ICOs represent a democratization of investment, in effect a form of crowdfunding, where individual investors can support the development of blockchain solutions that they would like to see succeed, rather than intermediaries, such as bankers, venture capitalists and executives of large companies acting as gatekeepers as to which ventures get funded.[2] The ability of companies to raise so much money, so rapidly, through ICOs, is, to a large extent, enabled by the evolving nature of ICO regulation around the world. Many offerings effectively take place in relatively unregulated markets without the offerings necessarily being vetted or endorsed by knowledgeable and trusted intermediaries. Investments in coins issued through an ICO, either through the ICO, or subsequently on a cryptocurrency exchange, represent a high risk for investors, due to the early stage of businesses raising funds, experimentation around blockchain business models, and this lack of regulation.[2] Not surprisingly, many of the previous ICO raisings have failed. Regulators around the world are developing regulation more aggressively, examining the behavior of founders and promoters, introducing regulatory certainty for companies looking to go down the ICO path.

This book chapter is structured as follows: traditional sources of entrepreneurial finance are described, along with the advantages and disadvantages of each, followed by a discussion of the more recently emerged crowdfunding, in order to identify the challenges of funding an entrepreneurial venture. Blockchain technology and emerging blockchain business models and types of tokens/coins are discussed briefly, in order to introduce ICOs as a form of entrepreneurial finance and the ICO process. These topics are covered in much more detail in other chapters of this book. Regulation of ICOs will be touched on briefly, as regulation differs around the world and is evolving rapidly, but impacts on the ICO process and the ability of companies to raise funds via this source. The potential advantages and disadvantages of ICOs for both entrepreneurs and investors are identified, and compared to other sources of entrepreneurial finance. We review the ICO performance literature as an understanding of what makes a successful ICO important to both blockchain entrepreneurs and potential investors. Finally, we conclude by making some very tentative suggestions on how the field may develop in the future, and suggest future research.

2. Entrepreneurial Finance and Traditional Sources of Finance

Entrepreneurial finance, the intersection between entrepreneurship and finance, [3] is crucial for early-stage businesses to fund the establishment and growth of the business. [4] Early stages of business can be capital-intensive requiring the development of products and services, establishing premises, and hiring staff ahead of the generation of sufficient revenues to fund these investments. [5] This early stage can also be relatively risky, particularly when the service is new to the market, a new business model is being implemented, or the founders have minimal experience in starting and/or running a business. Research has found that the survival rate of new technology ventures with five or more employees is only 21.9% after five years. [6]

While there are many sources of finance for established and larger companies, choices for entrepreneurial, early stage companies have traditionally been much more limited, due to the risk involved and the lack of a track record. [7] Potential sources of finance expand as the business is proven, and uncertainty, and hence risk, are reduced. [5] [7] Financing methods differ on the risk to the founders, the degree of ownership the company gives up, the expertise provided by the funding source, and potential control given up. [4] The two main types of funding for early-stage companies are:

1. **Debt**: the borrowing of money, which generally requires payment of interest and repayment of the amount borrowed; and
2. **Equity**: where the funder receives a portion of ownership of the company. These new owners are entitled to a portion of any dividends paid out of profits, and can gain from increases in the value of the firm in the future. These new owners may have an influence on the management of the company.

An examination of traditional sources of entrepreneurial finance assists the understanding of ICOs and the role they can play for early-stage businesses. Table 1 describes these more conventional sources of finance, and their advantages and disadvantages.

Funding source	Key characteristics	Advantages	Disadvantages
Bootstrapping	- Founders use savings and personal debt, such as credit cards, mortgages, or personal loans, or accessing funds from friends and families through borrowing money or as investors. - Founders may continue to work in their day jobs and work on the venture part-time and may constrain investment by, for example running the business out of their garage.	- Founders have substantial skin in the game and wear the bulk of the risk, but also gain substantial returns if it is successful. This shows commitment to potential future providers of finance. - Limited access to funding can focus founders on the things that matter and encourage innovation in investing frugally.	- Limited access to funds where founders have low personal resources and only work on the business part-time can greatly constrain the speed at which the venture can be developed. This may be a big issue if speed to market is important. - The personal risk to founders is substantial. If the business fails, they still have to repay credit cards and personal loans and may lose their house.
Bank business loans	- Generally, not available to very early-stage businesses that do not have the cash flow or substantial assets to provide security over the loan. [8] [9] - As they grow, they may be provided access to loans, but the bank may demand director guarantees where if the business fails the directors are required to repay the loan.	- Where bank loans can be obtained it may enable more rapid business growth. - The loans are debt rather than equity, so the founders do not give up any ownership of the company and do not have to share future profits or increased value of the company.	- Founders as directors may remain personally liable for the loans if they give a guarantee and the business cannot repay the loan. - Debt increases risks to the business as interest and loan payments have to be made regardless of how the company performs.

			- The bank may provide limited expertise to the founders on managing and growing the business.
Angel investors	- High net worth investors that provide seed capital or early-stage finance to entrepreneurs. - Some angel investors have experience starting their own businesses and or managing companies and also provide advice and access to their business networks to the start-ups.	- Where equity finance is provided, the company does not pay interest. - Angel investors are aware of the need of the business for finance and often do not require dividends with the intent of gaining a return by selling their investment in a later round of financing when the value of the business has increased substantially. - The advice of the angel investor, access to business networks and potential credibility of being associated with the investor can be invaluable to the growing company.	- Angel investors remain relatively rare, so access is difficult. - The venture must be developed enough to enable potential investors to evaluate the opportunity. - Founders share equity or ownership of the business at relatively low valuations at the early stage of the business.

Venture capitalists	- Venture capital is a method of financing, where institutional investors selectively invest in early-stage businesses over a horizon of typically three to five years. [10, pp.3-5] - Venture capitalists are in the business of generating value for their funds by investing in growth businesses. - Venture capitalists typically have greater access to finance so therefore can make larger investments in early-stage companies than angel investors. - Venture capitalists will often have substantial experience in growing companies within their focus industries and take an active role in guiding the founders. - Typically, the achievement of targets is required at each stage before the venture capitalist will	- Access to funds and experience, knowledge and networks of venture capitalists can enable rapid growth and increase the value of the firm. - Association with well-known venture capitalists may increase the perceived legitimacy of the start-up in the market. - In addition, to the investment into equity, coaching is provided. [12, p. 691]	- Sell down of equity at an early stage at lower valuations. - More active management of venture capitalists can reduce founders' control of the business. - Venture capitalists may have an exit strategy, which requires founders to also exit the business. - Venture capitalists are highly selective, investing into one or two out of every hundred applications [10, p.5] and a rigorous due diligence process is undertaken. [13, p28, 14, p49]

	commit further funds. - Venture capitalists devote significant resources into understanding emerging technologies and markets, giving them the capabilities to deal with the challenges start-ups undergo. - Hybrid models consisting of VC-funding, followed by an ICO, are possible. With the support of the VC, a minimum viable product is developed and first traction can be shown, thus increasing the credibility of the start-up. [11, p5]		
Public ownership	- When firms get larger, they can potentially perform an initial public offering (IPO) to sell equity to the market. For doing so, the business has grown to a point, where the revenue and profitability warrant public ownership. - IPOs are conducted when a company is going public,	- The potential to raise a large amount of funds from a broad base of investors. - Shares can be traded on the Stock Exchange making them more liquid and increasing attractiveness to investors.	- This is only suitable for companies that have been successfully operating for a few years. - To IPO, the business has to undergo significant changes and the process is expensive (cost of the process and substantial

	aiming to be listed on a stock exchange. [15, p3] - While rules are different across countries and stock exchanges, companies generally require a history of operations before they can IPO.		regulatory costs) and time-consuming. [16, p265]

Table 1: Mainstream Funding Sources for Early-stage Ventures [4] [5] [7]

In addition to these market-driven sources of finance, early-stage companies can sometimes qualify for government incentives or grants.

In summary, these traditional forms of entrepreneurial finance are difficult to access, and can be limited in the amount that can be raised early in a company's lifecycle, slowing the speed of growth. These sources of funding can require founders to commit all personal resources, and expose them to liability to repay the debt even if the venture fails. Selling equity in the firm to specialists, such as angel investors or venture capitalists, can provide access to valuable knowledge and networks, but dilutes ownership and control at relatively low early valuations. The internet has enabled the emergence of new sources of funding.

3. The Emergence of Crowdfunding as a Source of Finance

Crowdfunding emerged over recent years as a way for entrepreneurs to raise funds. Crowdfunding resembles a novel source of financing, and refers to entrepreneurs raising funds from many individuals, each making a small contribution. Crowdfunding platforms enable small amounts of money to be raised from many individuals to raise significant funds. [7] [17] Crowdfunding platforms, such as Kickstarter, take an essential role as an intermediary. [18] Primarily, two forms of crowdfunding exist, which are either reward-based or equity-based/investment-based. Both usually require a platform as an intermediary, who has a vested interest to select credible projects. [13] [26] However, in recent years, additional forms of

crowdfunding (donation-based and lending-based) have emerged. Table 2 outlines the key characteristics of the different types of crowdfunding.

Types of crowdfunding	Key Characteristics
Donation-based crowdfunding	- Individuals or not-for-profits post a proposed project and target a fundraising amount on a crowdfunding platform, such as Kickstarter.com. - Members of the general public can elect to contribute to the project if they would like to see it proceed. - Contributed amounts are effectively a donation, with those contributing not receiving any other benefits.
Reward-based crowdfunding	- Entrepreneurs can pitch their business idea to the public, via crowdfunding platforms. - Those contributing receive a reward for contributing based on the amount contributed. E.g., this may be being sent one of the products being produced, or priority access to the proposed product. - Apart from raising funds to produce a new product, this enables companies to test demand for the product prior to committing significant resources to development and production. - Funds are raised without giving up equity or control.
Equity-based/investment-based crowdfunding	- Changes in legislation in some countries have enabled smaller privately-owned companies to raise capital through selling shares through crowdfunding. - This enables individuals to acquire shares in early-stage companies that are not yet publicly owned. - Equity-based crowdfunding is regulated with limits on the size of the companies that can do the fundraising, the amount that can be raised each year, in total, and by investor, and, in some countries, such as Australia, the requirement to do the raising through an accredited intermediary. - The process is more rapid and cost-effective than performing an IPO. - Shares are not listed on a stock exchange, so are quite illiquid for the investors.
Lending-based crowdfunding	- In some jurisdictions, the public can lend money to companies through crowdfunding platforms. - For companies borrowing money, this has the benefits of not giving up any equity or control, and provides access to debt funding.

Table 2: Main types of crowdfunding source [17]

In a reward-based crowdfunding campaign, consumers are invited to pre-order a product. The business aims to raise the capital needed to launch production. [19, 586] Further, the campaign can act as a form of market

research, validating the general interest in the entrepreneurial project, and providing potential future investors with valuable information. [20, p1608] Investment-based crowdfunding, on the other hand, is based on raising capital in exchange for equity securities or shares of future profits.[19, 586] Start-ups have to agree with the listing platform on a valuation of the firm. Based on the valuation and the capital needs, typically, a standardized financial contract is offered to the crowd on a first-come, first served basis. Rejection-rates of start-ups are high, as the platforms perform a detailed evaluation, selecting the most promising initiatives.[21, 151-152] Crowdfunding enables early-stage businesses to raise funds early in their lifecycle to establish and grow operations. While broad-based lending and equity can be raised through crowdfunding, other forms enable funds to be raised without giving up equity or taking on debt. Regulation has evolved in some jurisdictions to encourage equity crowdfunding, while protecting investors, through mandating processes, intermediaries, and placing annual limits on raisings. Investments are generally illiquid for investors without exchanges to enable trading of these securities.

4. A Brief Introduction to Blockchain

With new players from the non-banking sector having entered the financial market, [22, 241] they introduced new digital technologies, differentiating these players from traditional banks and enabling additional forms of financing. [23, 189-190] [24, 36] One emerging innovation in this context is blockchain, [25, 237] which is renowned as a distributed ledger technology and is expected to drive economic change globally, enabling trustworthy, transparent, fast, and secure solutions. [26, 15] The concept of blockchain was first outlined in a 2008 white paper written by Satoshi Nakamoto. The name is a pseudonym for an anonymous individual or group. [27] More recently, blockchain has been described as a giant interactive spreadsheet that everyone can access. The file is updated, and confirms that the digital transactions transferring funds are unique. [28, 1] In technical terms, blockchain is a decentralized and transparent ledger, where transaction records are shared by all network nodes. They are updated by miners and monitored by everyone, whilst no one owns or controls them. [28, 1] [29] In Figure 1, three key attributes of blockchain are shown.

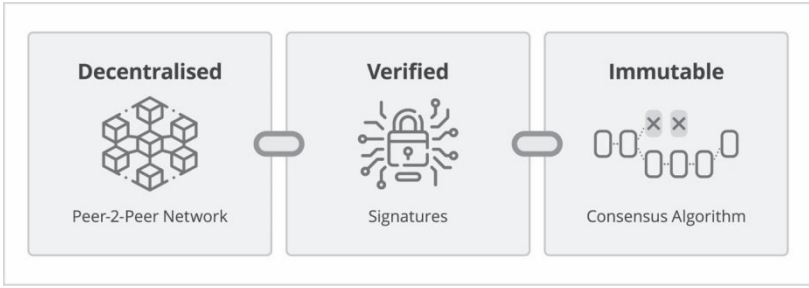


Figure 1: Key attributes of blockchain (Figure adapted[3] from [30, 5] using icons from [31] [32])

First, blockchain is decentralized, as the network is operated by its members, without a central authority being required. Second, each transaction is verified, as the members sign each transaction by using public-private-key cryptography. Third, the blockchain is immutable, as all members can verify transactions. In the case of no consensus being reached, blocks are rejected. Otherwise, if a consensus is reached, the block is added to the chain. [30, 5]

Based on blockchain technology, several applications, like cryptocurrencies, surfaced. They are a form of digital money, and appeared in 2009 with the introduction of bitcoin, founded by Satoshi Nakamoto. The main purpose of such digital assets is to be a medium in exchange, whilst using cryptography to ensure that all transactions are secured. [33, 106-107] Unlike traditional currencies, a centralized entity that produces the certified notes is not required. [34, 90] [35, 7] "No government or central authority can manipulate the supply, as it is governed by cryptographic rules, enforced by transparent computer code." [36, 33-34] People 'mine' the currency by making their computers' resources available to the cryptocurrencies network. Overall, cryptocurrencies, such as bitcoin, enable people to anonymously exchange goods and services electronically without relying on third parties, such as banks. [37, 106]

5. Initial Coin Offerings

The emergence of ICOs, (Initial Cryptoasset Offerings or Initial Token Offerings [38] or Token Generation Event [39] or Token Sale of Cryptocurrency Coins [40]) as a new means of democratizing and decentralizing capital access and capital formation for new crypto

ventures, [41] or open-source blockchain-type start-ups, [42] allows, through its different functions, the development of communities, while building powerful and effective network externalities through crypto-tokens, e.g. bitcoin or Ether, with a variable and volatile exchange rate, with fiat currencies. [43, 44]

5.1. Understanding the Domain

In 2012, this concept was opened up to the field of entrepreneurial finance, with J.R. Willet publishing "The Second Bitcoin Whitepaper". [45, 170] He hypothesized that money for computer science projects could be raised by creating a coin that is used by that project. This type of fundraising is a novel form of crowdfunding, where existing cryptocurrencies are exchanged by participants for entity-specific crypto-tokens. [46, 247-251] It is known as initial coin offering (ICO). ICOs have been vastly associated with crowdfunding, regulatory, and government policies, cryptocurrency and virtual currency markets, private equity and securities, commodities, and fraud.

In the subsequent year, Vitalik Buterin developed a concept to further extend the capabilities of bitcoin. [47] Instead of focusing on a digital cash system allowing payments, Ethereum resembles a general-purpose blockchain, running decentralized applications. [48, 9] It is capable of supporting smart contracts, which are agreements whose performance is automated. [49, p120] As such contracts exist in the form of written code, they allow for storing rules based on 'if, then' conditions, which can self-execute, thus enforcing the management and performance, as well as the payment, of the underlying contract. [50, 26-27]. Roose (2019) describes ICOs as follows:

> "Imagine that a friend is building a casino and asks you to invest. In exchange, you get chips that can be used at the casino tables. Now imagine that the value of the chips isn't fixed, and will instead fluctuate depending on the popularity of the casino, the number of other gamblers and the regulatory environment for casinos. Oh, and instead of a friend, imagine it's a stranger on the internet who might be using a fake name, who might not actually know how to build a casino, and whom you probably can't sue for fraud if he steals your money and uses it to buy a Porsche instead. That's an ICO." [51]

The first ICO was conducted by Mastercoin via a forum thread announcement on bitcointalk.org in 2013. It attracted 551 anonymous contributors investing 4.740 bitcoin. [53, 7] One year later, the ICO of

Ethereum raised 3,700 bitcoin, worth US$ 2.3 million, within the first 12 hours. [54] The Toronto-based project worked together with lawyers from the Swiss consulting-firm MME, to develop a fundraising method, establishing a charitable foundation in Switzerland. Throughout, the ICO received a total of US$ 18.3 million in donations. [55] The amount of money raised per ICO increased in subsequent years, and peaked in 2018 with US$ 4 billion being raised for the project EOS. [57] Many people invested in this platform, which wasn't yet live, based on hype, and the promise that the well-known blockchain-project founders would repeat their success. The objective of EOS is to support more efficient operations for decentralised applications, thus making it a competitor to Ethereum. [58]

During the last couple of years, various business models have received funding from ICOs worldwide. Some notable business models include: scalable smart contracts (EOS); encrypted messaging, and blockchain ecosystem (Telegram): decentralized currency for casinos (Dragon); cryptocurrency exchange (Huobi); IoT contract and payment platform (Hdac); decentralized cloud storage (Filecoin); self-amending distributed ledger (Tezos); open-source blockchain smartphone (Sirin Labs); prediction markets (Bancor); decentralized investor-driven venture capital fund (The DAO); 'tokenising labour hours' that allow workers to be paid via cryptocurrency through a decentralized platform (Chronobank); providing greater visibility to farmers and grain brokers over their supply chains through a blockchain-based logistics platform (BlockGrain); democratized voting on the Blockchain (Horizon State): crypto-focused online freelancing marketplace (CanYa); and using blockchain technology for households to trade surplus solar power (Power Ledger).

The abovementioned diverse business models have used various distributed platforms connecting investors and investees, unfolding a democratization paradigm in investment and fundraising. The network externalities generated provide community-based pathways for fostering entrepreneurial innovation by leveraging on the power of the crowd, along with utilizing technological breakthroughs for the development of diverse and novel business models.

5.2. ICOs and other Sources of Entrepreneurial Finance

ICOs are utilized by early-stage start-ups, which might not even have the necessary operations established yet. [13, 24] In addition, ICO firms don't require an underwriter to determine value [59, 2] and they bypass banking

and non-banking entities, making ICOs ten times less costly than IPOs. [60, 1118] Further, no shares of the issuing legal entity are acquired in an ICO, meaning investors do not establish a direct involvement in the business. Therefore, the equity of the business is not diluted. [11, 3] [60, 1119] [61, 85] This form of financing is similar to reward-based crowdfunding, as it is appealing to individuals, the investments occur towards a product or service, and equity is not diluted.[62, 124] In contrast to crowdfunding however, in an ICO, a presell product does not have to be built, and a price commitment to the future product is not required.[13, 26-27] In equity-based crowdfunding, investment decisions are largely, but not totally, based on financial return motivation and investors are provided with reviewed fundamental data, which in this form is usually not available in ICOs. [13, 27]

Table 3 compares ICOs and other sources of entrepreneurial finance for both entrepreneurs of blockchain businesses and investors. These include initial public offerings (IPOs), venture capital (VC) and crowdfunding.

	ICO	IPO	Crowdfunding		VC
			Reward-based	Investment-based	
Stage	Early Stage	After Series D	Early Stage		Early Stage
Type	Project	Business	Project	Business	Business
Speed of Execution	Quick	Slow	Quick	Medium	Slow
Investors	Unlimited	Restricted	Unlimited		Restricted
Valuation	None	Fundamental	None	Fundamental	Fundamental
Regulation	None	Yes	via Platform		via VC
Equity Diluted	No	Yes	No	Yes	Yes

Table 3: Comparison to alternative sources of financing [10, 3-4] [11, 5] [12, 691] [13, 26-29] [19, 586] [21, 151-152]

5.3. The ICOs Marketplace

Overall, the ICO market underwent a significant transformation in recent years, and is continuously tracked by various websites. Most of those are

curated manually, as there is no compulsory platform or register for ICOs. [63, p3]

The number of ICOs increased through 2017 and 2018. An estimated 91 ICOs occurred daily in 2017, while the number increased to 482 in the subsequent year. Meanwhile, the annual amount invested rose in the same period, from US$10 billion to US$11.4 billion, and the first ICO unicorns emerged in 2018, with EOS and Telegram. [1] [64, 3] As mentioned above, over recent months, ICOs have fallen from the highs of 2018. Over the time of observation, the US, Switzerland, and Singapore, remained the key global ICO-hubs. In 2018 however, the concentration decreased, and the UK and Hong Kong gained significant ground. Additionally, new ICO-friendly jurisdictions surfaced in countries like Liechtenstein, Malta, and Gibraltar, positioning themselves with interesting offerings for ICOs. [1] [64, 3-7] [65, 10]

Since mid-2018, the number of ICOs, as well as the funded volume, decreased, leading to a crypto-winter. [66] One reason for this development was the tandem effect of the market. Bitcoin was volatile and decreased in value, affecting Ethereum (which fell from its yearly high of US$1,342 to US$84). As a result, investors became less likely to buy into ICOs, leading to a market slow-down. [1] [67] Another reason is shown by a study conducted by EY. The study monitored ICOs over the two-year period, and concluded that 86% were listed below ICO price, and 30% of ICOs showed substantial losses. Further, 71% of businesses still didn't have an offering in the market, which is high compared to venture-backed firms. [68]

As a result, investors started looking into doing more due diligence, searching for more credible and vetted projects. [67] It led to the development of security token offerings (STOs), which are a more regulated form of ICOs. They combine the low entry barriers of ICOs with traditional fundraising characteristics, including know your customer (KYC) and anti-money laundering (AML). [66] In an attempt to address the quality and legitimacy issues, some crypto exchanges (also known as 'launchpads') are now vetting and offering initial exchange offerings (IEOs), although some have questioned the quality of the exchanges vetting process. [69] By definition, an IEO is a crypto-enabled financing scheme administered by a well-known, trustworthy, and established cryptocurrency trading and exchange platform (e.g. Upbit, Bithumb, Binance, OKEx [OK Jumpstart], KuCoin Spotlight, Huobi Prime, Bitmax Exchanges, Bittrex International IEO, Paytomat). Registered users have

the ability to purchase tokens using funds that are available in their respective exchange wallets (fiat or cryptocurrencies). Latest figures for the period (January 1 2019 - April 30 2019) show that 14 IEO projects have successfully raised approx. US$166 million of cryptocurrency-based funding globally.([4]) Contrary to ICOs, IEOs are administrated by a counterparty([5]) and the crypto tokens are not publicly available. Users who are registered within the respective exchange platform (reducing anonymity) have the opportunity to participate in an IEO fundraising event. That means that the third-party exchange platform serves as an additional auditing layer (KYC/AML verification) screening both token issuers and investors so as to minimize fraudulent actions.

Ultimately, the question arises, whether ICOs are innovative. Schumpeter defines innovation as "the doing of new things or the doing of things that are already done, in a new way." [70, 13] Further, these new objects, methods or ideas, have to be successfully implemented in a market. [71, 26]

As ICOs are an application of crowdfunding, they are not a new method of financing. However, utilizing blockchain technology to automate the settlement process between the involved parties is a novelty. As previously outlined, more than US$20 billion were raised until the end of 2018 through ICOs, [72] and the ICO landscape is transforming, thus showing that ICOs are an innovation.

5.4. The ICO Process

Before conducting an ICO, the issuing business typically publishes a white paper, providing information about the entity and the project, the rights associated to the to-be-issued token, and how the sale proceeds. [73, 44] Afterwards, a presale takes place, in which large investors and people close to the project participate. Finally, the actual ICO occurs at an announced date, and the general public gains access to the tokens offered. [74, 5]

Two smart contracts are created. In these, a set of variables, such as total funding accepted, duration of the ICO, price of the issued tokens, and amount of coins distributed, are defined. After the smart contracts become available, investors pay funds towards the ICO smart contract, triggering an automated process, through which the project gains access to the funds paid into the contract. Further, the investor receives the number of tokens purchased. [75, 3]

According to the US Securities and Exchange Commission (SEC), there are two types of tokens: a) security tokens; and b) utility tokens. In the US, the Howey test is used to determine whether an investment is a security, i.e. a crypto token to be considered as a security token. This includes "whether the investor has an investment of money made by the purchaser, whether the investment is part of a common enterprise among numerous investors, and whether the success of the enterprise depends on the efforts of the third party promoter…whether the investor has an expectation of a financial return." [76, 16] Security tokens are subject to mainstream regulatory provisions, and since the majority of ICOs are investment opportunities, the crypto tokens are treated as security tokens (capital markets products). On the other hand, utility tokens are the crypto tokens that do not pass the Howey test. This category of crypto tokens aims at providing users with a product, a service, or both. The US Securities and Exchange Commission([6]) has recently stated that:

> "ICOs, or more specifically tokens, can be called a variety of names, but merely calling a token a 'utility' token, or structuring it to provide some utility, does not prevent the token from being a security."[77]

The abovementioned statement provides a new taxonomy on security tokens, which can have three forms: a) payment tokens (payments and/or means of money/value transfer); b) utility tokens (providing access to a decentralized platform or respective service); and /or c) asset tokens (representing assets or rights, such as debt or equity).

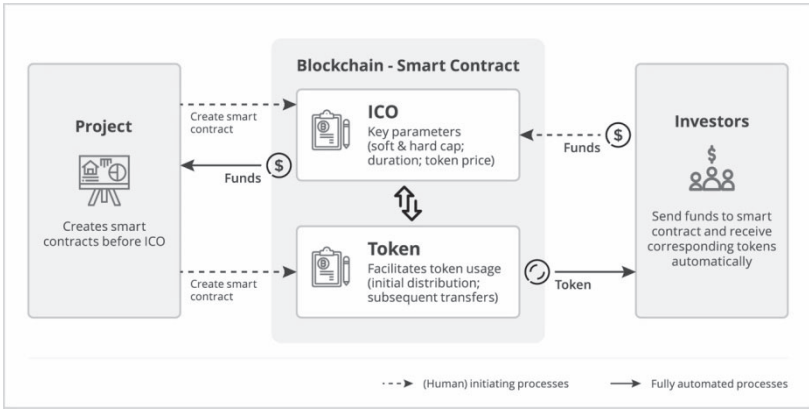


Figure 2: ICO Process (based[7] on [75, 3] using icons from [78–81])

Typically, ICOs are conducted by companies in the earliest life cycle stage. [59, 2] By doing so, they fundraise directly, bypassing banking and non-banking entities. This makes ICOs ten times less costly than IPOs.[60, 1118] Meanwhile, a worldwide potential pool of investors is attracted. [11, 4] [60, 1119] They benefit from low barriers of entry, gaining access to high innovative ventures, which would not be possible otherwise. [60, 1118] Further, investors are attracted by the easiness of transferring funds through blockchain transactions, whilst hoping for very high returns.[82, 26] [83, 24] As the white papers often contain clichés, they particularly attract inexperienced investors. Overall, these factors contribute to the ICO-market being highly volatile, as valuations of projects are based on the fear of missing out, instead of fundamentals, such as discounted cash flows. [84, 2-11] As a result, projects are under high speculative pressure from the moment of listing. [11, 4]

Next to ICOs, businesses occasionally conduct airdrops, in which existing holders of a particular cryptocurrency receive tokens of a newly-created currency for free. Hereby, a wider distribution is achieved, leading to higher mindshare and engagement of crypto-holders. [85, 141]

6. Regulatory Considerations

The rapid growth of the blockchain-enabled entrepreneurial financial funding space, the decentralized cryptocurrency-related investments landscape, and the overall crypto economy capital market, illuminate numerous risks, and regulatory and accountability challenges which are gradually beginning to be addressed by regulators across the globe. Policymakers and regulators around the world have not yet reached any consensus in relation to the ways of developing legal frameworks for ICOs and STOs.

The absence of regulatory constraints and procedures, along with disaggregated approaches towards understanding, defining, and categorizing this new funding mechanism, prove substantial, and amplify hurdles towards establishing a harmonized regulatory and cross-jurisdictional framework which will protect the investors and other marketplace participants against ‘scalping’, ‘spoofing’, ‘fraudulent’, ‘pump and dump’, and other manipulative practices, [86] [87] on the same level as of traditional securities markets, while at the same time enabling a successful widespread adoption of this innovative channel of capital access and capital formation. Moreover, it shows that current regulatory

practices are ill-equipped to handle these new blockchain-enabled entrepreneurial finance mechanisms.

The transformative and disruptive technological developments behind ICOs, the heterogeneity of products and participants, and the overall emerging ecosystems (local, national, and international) that are developing around this funding mechanism, call for revisiting and reconceptualizing regulatory and accountability aspects, in light of numerous scam ICOs campaigns promising 'easy profit' or guaranteed returns to investors, particularly due to lack of regulatory compliance requirements and cybersecurity threats.

Frequent cases of information asymmetries in dubious and 'dodgy' white papers, often published by anonymous and untraceable issuers, without high-quality standards assurance, and lack of governance mechanisms, pose substantial threats and risk transferred to investors who find themselves being engaged with speculative investments. This calls for increased regulatory oversight and protection against these vulnerabilities. [41] These information asymmetries usually result in investment decisions that cannot be based on a rational calculus. [88] The provision of credible and trustworthy information via an ICO white paper can minimize, or even eliminate, information asymmetries, ensuring the protection of interests and rights of the involved cohort of investing stakeholders, along with the long-term viability of the respective mechanism. [89]

ICO tokens fall under pre-determined regulatory mechanisms, accompanied by important disclosures, processes, and other associated investor protections, only when they are classified as tokenized securities. [86] These equity/asset tokens provide a right to a promised future cash flow generated by the underlying business. However, there is still an on-going debate in relation to the utility or access tokens classification stream, due to the underlying utility characteristics and the uncertainty amongst regulators and policymakers towards determining which ICOs are subject to which financial markets regulation. [90] The latter type of token provides the right to access a future product or service, a characteristic that could potentially classify it as managed investment.

Typically, an investment in a conventional venture/business is accompanied by a cohort of legal and enforceable rights. For a shareholder, this is translated to dividends; for a lender it is translated to interest or share in case of default or insolvency. By design, cryptocurrencies are resistant to regulation and censorship, [91] primarily

due to their virtual and internet-base, and thus their world-wide nature. [90] [92] This increases the regulatory uncertainty behind ICOs, since this mechanism does not fall within predefined and mainstream regulatory procedures. [41] The US Securities and Exchange Commission[8] has recently stated:

"Recognize that these products are often sold on markets that span international borders and that significant trading may occur on systems and platforms outside the United States. Your invested funds may quickly travel overseas without your knowledge. Although the SEC actively enforces securities laws, risks can be amplified, including the risk that market regulators may not be able to effectively pursue bad actors or recover funds." [77]

Most ICOs have been structured to attempt to avoid being classified as securities, by requiring payment in other cryptocurrencies rather than money, avoiding a sale of equity and any mention of dividends (i.e. the sharing of profits). ICOs though, are still subject to consumer and trading laws targeting misleading conduct. [93] The US is taking actions on scam ICOs through prosecuting ICO promotors for wire fraud. In this context, even where the securities law does not apply, there are laws against fraud and misleading conduct (consumer laws) under which regulators are acting. In a similar manner, the Swiss Financial Market Supervisory Authority (FINMA) considered a US$90 million ICO as illegal, due to the fact that the company issued bond-like tokens without a license, along with information asymmetries and lack of internal auditing capabilities. The Singapore Exchange Regulation (SGX RegCo) has recently announced requirements for listed companies which are planning to conduct an ICO, clarifying that even if an SGX-listed company is the issuer of digital tokens, those tokens are not listed on SGX, therefore SGX rules cover neither the token-holders nor the tokens. These examples highlight the fact that regulators are taking a much closer and comprehensive look into ICOs, and are ready to apply mainstream and traditional legal instruments and rules to cryptocurrency-enabled fundraising.

Still, the dissemination of information, use of funds and regulatory compliance of an ICO campaign falls under the control of the issuer/promoter/entrepreneur. [94] In this context, the perceived trust between the investor and the issuer/promoter is exclusively based on the legitimate behavior of the venture which promises certain rights to the investors (who are responsible for conducting their own due diligence and

information validation), in exchange for funding; rights that investors do not have the means to legally enforce, if required. [42] Within digital entrepreneurship, the establishment of this level of trust is very important, since it can facilitate innovation activity and knowledge spillover. [95] Crypto exchanges are now stepping in to adhere these issues through IEOs where the issuance is vetted and underwritten by the exchange, [69] leveraging the expertise and reputation of the exchange. This creates a further regulatory risk of the offerings being seen as securities, and the exchanges as broker-dealers. [69]

According to [96] there are three types of regulatory regimes for the ICOs marketplace: a) open and liberal; b) cautious but still open; and c) strictly ban ICOs. A number of regulators and governments worldwide believe that smart and concise regulation of ICOs could potentially bring advantages (speed, lower-cost form of fundraising) for the entrepreneurs who wish to retain full equity of their ventures. Within the continuous endeavor to successfully strike a balance between innovation and protection, while overcoming the abovementioned shortcomings, a number of regulators (Estonia, Singapore, Australia, United Kingdom and Switzerland) try to formulate coherent regulatory frameworks by adopting a 'case-by-case' or 'relative-to-a-function' approach towards legitimizing ICOs, under the caveat that cross-jurisdictional solutions may not be feasible. [92] Switzerland has begun treating ICOs as securities, resulting in applying laws and rules that are used within the traditional capital markets regulatory frameworks. The application of securities law and any other banking or financial legal provisions depends on the specific contextual and structural (security, loan, voucher, currency) peculiarities, [92] The recently-published Issues Paper by The Australian Government Treasury states that:

> "Future growth in ICO popularity could potentially create competition with traditional forms of fundraising, generating greater efficiencies across the financial system. So long as the incentives faced by fundraisers and investors are sufficiently aligned, ICOs could help to improve the efficiency of capital allocation and contribute to economic growth." [97, 6]

The Australian Transaction Reports and Analysis Centre (AUSTRAC) has begun implementing new anti-money laundering and counter-terrorism financing (AML/CTF) laws for digital currency exchange (DCE) regulating service providers of cryptocurrencies. Exchange platforms operating within Australia are required to register with AUSTRAC and be in compliance with the respective Australian AML/CTF obligations. In

this context, financial penalties and criminal charges will be imposed on unregistered exchange platforms. At the same time, the Australian Taxation Office (ATO) is strengthening intelligence capabilities by collecting information (data matching) from Australian Cryptocurrency Designated Service Providers (DSPs), towards ensuring compliance in terms of taxpayers that trade in cryptocurrencies, to correctly and diligently disclose income details so as to concisely meet their respective tax obligations, along with fighting tax evasion and money laundering practices.

Some regulatory authorities (China, India, South Korea) have taken a very firm stance, having banned any ICO activities, and threatening severe punishments and stern penalties, along with requiring that funds be returned to investors (Chinese and South Korean authorities). In particular, the Chinese National Internet Finance Association raised warnings against ICOs, which are considered as a financial risk and potential disruptors of the socio-economic order. Other regulatory authorities (United States) place emphasis on issues which investors can be faced with, such as money laundering, financing terrorism, and fraud, along with imposing heavy regulatory requirements across states. Moreover, the US Securities and Exchange Commission[9] has taken into account that a number of ICOs could be considered as securities.

> "ICOs can be effective ways for entrepreneurs and others to raise capital. However, the novel technological nature of an ICO does not change the fundamental point that, when a security is being offered, our securities laws must be followed." [98]

An interesting form which is currently emerging is 'self-regulation', where automated compliance and monitoring is conducted by market participants [87] in order to distinguish genuine fundraising activities through ICOs against scams. In general, the peculiarities of the ICOs marketplace will be better accommodated and integrated within a well-developed digital regulation environment. [99]

7. The Entrepreneurs' Perspective of ICOs

The above analysis suggests that ICOs offer substantial advantages and disadvantages to entrepreneurs seeking to start and grow a blockchain-related business.

7.1. Potential Benefits of ICOs for Entrepreneurs

- **Early stage of fundraising:** Using ICOs, entrepreneurs can potentially raise $millions when their blockchain solution is little more than an idea. Funds can be raised on the back of a white paper, which describes the planned technology solution and business mode. These funds are not available to entrepreneurs from other sources so early in the cycle. Venture capitalists can provide substantial funding, but phase funding is based on the entrepreneurs successfully proving their business model through funding gates. [4] IPOs provide high levels of funds, but require the business to have been successfully operating for years.

- **Enabling blockchain businesses to get tokens in the hands of, and incentivize, key industry players:** Blockchain solutions often are network solutions where the value to any participant is dependent on other participants on the platform. [2] [76] Presales or airdrops of coins to key stakeholders, with the potential of increased value on ICO, may motivate them to join and support the platform and promote the ICO, building the required network effect.[2]

- **Enabling customers to participate in growth in value, and issuers to gauge demand:** This is the democratization of investment opportunities, but also provides early insight as to whether there is sufficient demand for the product/service to be offered. [76]

- **Retaining equity:** Tokens sold through ICOs can represent a promise to provide a future service, rather than selling equity in the business. At early stages, angel investors and venture capitalists will place a relatively low value on the business, reflecting early stage risk, so substantial fundraising will require a significant portion of the equity in the business, requiring founders to share profits and capital growth.

- **Retaining control:** As ICOs don’t give up equity, founders retain control of the business.

- **Avoiding taking on personal or business debt.**

- **Lack of regulation:** Current regulatory gaps enable entrepreneurs to raise funds broadly without the constraints and costs of regulatory red tape. This includes limited, if any, requirements for ongoing reporting to investors.

- **Speed and cost-effectiveness of fundraising:** ICOs can still make substantial management efforts and involve significant investment, however, these are significantly less, compared to an IPO. The speed and facilitation of network effects are important, and may be easily imitated. [76]

7.2. Potential Limitations/Issues of ICOs for Entrepreneurs

- **ICOs are only appropriate for businesses with a blockchain solution,** limiting the applicability of this funding source for other entrepreneurial ventures.
- **Risks associated with blockchain businesses**. Early stage, unproven business models and the network effect, requiring substantial stakeholder participation.
- **Documenting business and technology plans in advance,** in the white paper, can make agile development and 'pivoting' the business difficult for those that try to honor promises made and continue to engage with token holders.
- **Evolving regulation and regulatory uncertainty**. When the token is not considered a security, while securities regulation may be avoided, the ICO may be considered a sale of a product, which is subject to tax, whilst issuing securities are not. [76]
- **Cybersecurity risks** with an estimated 10% of the coins issued or proceeds of ICOs stolen from exchanges and hacking, spoofing sites. [84]
- **Volatility and lower prices for cryptocurrencies, tokens and coins,** with the market well down from the peak in December 2017 and January 2018.
- **An increasing number of failed previous offerings** affecting the reputation of the funding source, and potentially the future willingness of investors to fund new businesses through these mechanisms.
- **Reducing information asymmetries as investors gain greater knowledge** of blockchain businesses and ICO dynamics.
- **Future fundraising may impact on the value of previously-issued coins** reducing future funding flexibility for issuers. [100]

8. The Investors' Perspective of ICOs

As previously discussed, ICOs provide a significant potential benefit to entrepreneurs seeking to raise substantial levels of funds globally, directly from private investors, in order to finance blockchain projects from an early stage. The other side of this transaction relates to the many individuals around the world investing in these projects. Participating in ICOs has some potential benefits and issues/ risks for investors, as discussed below.

8.1. Potential Benefits of ICOs for Investors

- **ICOs provide individual investors with the ability to provide funding** to enable blockchain projects that they value to be developed and implemented. For virtually unregulated reward-based ICOs, this is true democratization of the investment process, with the elimination of gate-keepers determining which potential projects should be funded. [2]
- **ICOs provide individual investors with the opportunity to invest at a much earlier stage** in the project before most other forms of investment.
- **Many tokens issued in ICOs are listed on cryptocurrency exchanges,** providing liquidity to the investments and enabling investors to track their value. This liquidity does not generally exist in other forms of crowdfunding, including equity-based funding where shares are not listed on exchanges.
- **Early investment and past boom times in the ICO market enabled some investors to realize substantial gains** in the value of their tokens.

8.2. Potential Issues and Risks of ICOs for Investors

While opportunities for investors in ICOs are potentially high, the potential issues and risks are substantial. These include:

- **Most ICOs are reward-based not equity-based:** It is not always clear what investors are getting for their money. By buying tokens, investors may not be gaining any ownership of the company issuing the tokens. Tokens may entitle the owners to future services on the platform, but what is the value of those services?

- **The early stage of the investment carries substantial risks:** Many ICOs are little more than an idea documented in a white paper, with 84% at the ideas stage, 11% with prototypes, and 5% running projects. [84] Rigorous business cases may not yet have been developed, markets and brand-new business models may not yet have been tested, technical problems may be encountered, key industry stakeholders may not yet be on board, and managers may not have a track record. What could go wrong? Most organizations that perform ICOs will fail, making coins acquired through the ICO worthless.

- **Blockchain-related businesses are a new area for both entrepreneurs and investors:** There is little evidence yet as to the types of blockchain models that will be successful and those that won't, and how best to develop them. Investors have little experience in evaluating successful models. This suggests that there will be substantial trial and error (and failures), and that the errors will receive funding, creating losses for investors.

- **Relatively low barriers to entry at least to the ICO stage:** The early stage of the ICO means others can relatively quickly develop a competing offer white paper, impacting the value of tokens of early movers.

- **Tokens may fall in value if too many are created:** If the supply of tokens exceeds the demand, inflation may reduce the value of tokens held by investors. [100]

- **Cybersecurity risks:** An estimated 10% of ICO proceeds are lost through hacker attacks with investors' personal data, as well as, funds at risk. [84]

- **Lack of regulatory protection**: The lack of regulation creates access for individuals to invest in ICOs and the democratization of the investment process. However, it creates substantial risks to investors including exposure to poor quality offerings, fraudulent ICOs, 'pump and dump' schemes, and lack of protection once invested.

- **Risk of regulatory change**: There is the potential that future increased regulation could impact the ability of token owners to sell.

- **Lack of intermediaries providing some assurance of quality**.

- **A falling cryptocurrency market may dampen demand for tokens**: Significant past ICO fundraising may have been driven by the staggering increases in the values of major cryptocurrencies, such as bitcoin and Ether, through 2017. Since the peaks in December 2017 and January 2018, as of 12 March 2019, bitcoin is 91% below its peak of almost US$20,000 (December 17 2017) and Ethereum is down 81% from its high of US$1,422 (January 13 2018). Ether is up 58% since a low on 15 December 2018). Bitcoin is up 19.4% since a low on 16 December 2018.

9. Determining ICO Performance and what makes a 'good' ICO

Blockchain businesses and the ICO market have emerged too recently to analyze long-term financial performance for firms or investors. Developing and implementing the solution, and building a sustainable network, may take years. There have been some studies on the success of ICOs from the founders' perspective where success has been defined as successfully raising funds, [101] the amount of money raised, [63] and the token liquidity. [76] All these studies suggest that the ability to raise funds is affected by factors such as, length of the white paper, [63] [76] provision of high-quality blockchain code, [63] [76] [101] when a token presale is organized, [76] [101] and when tokens enable holders to participate in a specific service or share profits. [76] [101] Prior VC equity involvement, and an entrepreneurial professional background for the lead entrepreneur, affect liquidity and trading volumes, but prior experience in the crypto community, computer science or finance do not. [76]

Apart from the early stage of development of blockchain solutions underlying ICOs, assessing the success of ICOs from the perspective of other stakeholders is made more challenging, as investors may have reasons other than financial returns for investing in the ICO. This could include enabling a worthwhile project to be developed, intending to utilize coins issued in ICO to participate on the platform post-ICO, expectations of long-term financial returns, or speculation on increases in market value of issued coins.

While assessing long-term success for ICO investors may not yet be possible, some work has been done to explore short-term performance.

Analysis identified that, as of the 2 September 2018, 86% of tokens issued in 2017 ICOs were below their issue value, 30% had lost virtually all of their value, and a portfolio of tokens from 2017 ICOs acquired on 1 January 2018 had lost 66% of its value. [68] Only 29% had a working product or prototype. [68]

10. Concluding Remarks

The crypto ecosystem is still nascent, and within its early stage of development. ICOs have proven to be an innovative new form of entrepreneurial finance, which has enabled many new blockchain ideas and business models to be funded at an early stage of development. By enabling the public to choose which ideas are funded, ICOs democratize investment and potentially enable the emergence of solutions with social, as well as, economic benefits.

ICOs can make substantial funds available to blockchain enterprises at a stage when entrepreneurial finance is difficult to access, which enables funds to be raised without giving up equity or control of the business. However, ICOs represent risky investments for members of the public investing in them, due to the early stage of blockchain businesses issuing coins, the untested nature of blockchain business models, the exclusion of knowledgeable intermediaries in the process, and regulatory gaps. The Organization for Economic Cooperation and Development (OECD) in the recently-published Initial Coin Offerings (ICOs) for SME Financing report states:

> "It therefore seems inappropriate to consider ICOs as a potential 'mainstream' financing mechanism for SMEs whose projects are not enabled by DLTs and which would not benefit from network effects" [13, p39]

For ICOs to remain a long-term source of funding for entrepreneurial blockchain-related ventures, it is important that outcomes are good for investors, as well as those raising funds. The challenge for policymakers and regulators is to balance the benefits of innovation of, and be supported by, ICOs, protecting the interests of investors. Limited regulation, or outright banning of ICOs, as exists in some jurisdictions, is not likely to achieve this balance. Regulators in jurisdictions that have taken a 'wait and see' approach on ICOs, such as Australia and the US, have recently become more active in prosecuting fraudulent behavior, preventing 'shonky' fundraising and consulting on appropriate regulation.

In our view, regulation will increase, but will seek to retain broad access to investors and maintain a manageable regulatory burden. This may look something like equity crowdfunding regulations, requiring appropriate disclosures, the involvement of registered or licensed intermediaries, and limitations on who can invest or the amount that can be invested by individual investors. The rise of IEOs is potentially a first step in this direction.

We suspect that much of the investor demand for ICOs has been driven by the rapid growth in the value of cryptocurrencies, such as bitcoin and Ethereum, through 2017, and the volatility in the prices of these assets since. Those that gained wealth were looking for the next bitcoin, while others suffered a fear of missing out, and hence, invested in new offerings. With the price of bitcoin now (as of mid-March 2019) around 20% of its high, much of the speculative froth may be removed from the ICO market. If the value of major cryptocurrencies remains static, or continues downward, the values of coins offered may be more reflective of the perceived value of the coins by participants in the blockchain offering, post-ICO.

Few, if any, blockchain-related businesses have been around long enough to show what business models, token structures, or other factors, are likely to contribute to success. Over time, we would expect greater knowledge to be accumulated by both founders and investors on blockchain business and ICO quality. More knowledgeable participants are likely to result in higher quality offerings, gaining a greater portion of funding and poorer quality fundraising failing to be supported.

The recent emergence of blockchain-related businesses, and the very recent explosion of ICOs, opens up potentially valuable streams of research. This includes exploring the nature and outcomes of blockchain-related businesses to identify outcomes, and the factors contributing towards the success or failure of these businesses for the founders, investors, and other stakeholders. This includes how the businesses successfully enrol key stakeholders onto the platform. The economics of these businesses, and how they generate returns for various classes of investors, including equity holders and other token owners would be insightful. As the ICO market is evolving around the world, it would be valuable to analyze performance, over time and across jurisdictions.

Endnotes

[1] Numbers can vary according to different reporting and data aggregation methods. E.g. The ICObench "ICO Market Quarterly Analysis Q1 2019" reports that 107 ICOs projects raised approx. US$ 902 million in that respective period of time. Available online at https://icobench.com/report?utm_campaign=im2019qr1901&utm_source=benchy#quarterly (Last accessed: May 1st 2019)

[2] Authors' calculations based on data received from https://icomarks.com

[3] Written permission to use an adapted and redrawn by the authors version of Figure 1: "Basic Properties of Blockchain" has been obtained.

[4] https://www.coinschedule.com/

[5] Jeff Dorman, Partner and Portfolio Manager, Arca Funds has commented that "The irony of course is that this is directly at odds with the decentralized ethos embedded in crypto, but this has been conveniently ignored as long as it's working. Everyone involved is highly motivated not to kill the golden goose"[69]

[6] https://www.sec.gov/ICO

[7] Written permission to use an adapted and redrawn by the authors version of Figure 1: "ICO Process" has been obtained.

[8] https://www.sec.gov/ICO

[9] https://www.sec.gov/news/speech/speech-clayton-120618#_ftn1

References

[1] D. Pozzi, *ICO Market 2018 vs 2017: Trends, Capitalization, Localization, Industries, Success Rate.* [Online] Available: https://cointelegraph.com/news/ico-market-2018-vs-2017-trends-capitalization-localization-industries-success-rate. Accessed on: Mar. 19 2019.

[2] Y. Chen, "Blockchain Tokens and the Potential Democratization of Entrepreneurship and Innovation," *Business Horizons*, vol. 61, no. 4, pp. 567–575, 2018.

[3] D. Cumming and S. Johan, "The Problems with and Promise of Entrepreneurial Finance," *Strat. Entrepreneurship J.*, vol. 11, no. 3, pp. 357–370, 2017.

[4] D. J. Denis, "Entrepreneurial Finance: An Overview of the Issues and Evidence," *Journal of Corporate Finance*, vol. 10, no. 2, pp. 301–326, 2004.

[5] J. C. Leach and R. W. Melicher, *Entrepreneurial Finance*. Australia, Mexico: Cengage Learning, 2018.

[6] M. Song, K. Podoynitsyna, H. van der Bij, and J. I. M. Halman, "Success Factors in New Ventures: A Meta-analysis*," *Journal of Product Innovation Management*, vol. 25, no. 1, pp. 7–27, 2008.

[7] G. E. Gibbons, R. D. Hisrich, and C. M. DaSilva, *Entrepreneurial Finance: A Global Perspective*. Los Angeles, California: Sage, 2015.

[8] D. J. Cumming and S. Vismara, "De-segmenting Research in Entrepreneurial Finance," *Venture Capital*, vol. 19, no. 1-2, pp. 17–27, 2017.

[9] M. Wright, T. Lumpkin, C. Zott, and R. Agarwal, "The Evolving Entrepreneurial Finance Landscape," *Strat. Entrepreneurship J.*, vol. 10, no. 3, pp. 229–234, 2016.

[10] D. Klonowski, "Venture Capital: A Closer Look Behind the Curtain," in *The Venture Capital Deformation*, D. Klonowski, Ed., Cham: Springer International Publishing, 2018, pp. 3–32.

[11] C. Hahn, *Initial Coin Offering (ICO): Unternehmensfinanzierung auf Basis der Blockchain-Technologie*. Wiesbaden: Springer Fachmedien Wiesbaden, 2018.

[12] A. Davila, G. Foster, and M. Gupta, "Venture Capital Financing and the Growth of Startup Firms," *Journal of Business Venturing*, vol. 18, no. 6, pp. 689–708, 2003.

[13] OECD, *Initial Coin Offerings (ICOs) for SME Financing.* [Online] Available: www.oecd.org/finance/initial-coin-offerings-for-sme-financing.htm. Accessed on: Mar. 17 2019.

[14] H. Landstrom and C. Mason, *Handbook of Research on Venture Capital*. Cheltenham: Edward Elgar Publishing, 2012.
[15] A. Khurshed, *The Investor's Guide to IPOs: How to Profit from Initial Public Offerings*. Petersfield: Harriman House, 2009.
[16] S. M. Bragg, "Initial Public Offering," in *The New CFO Financial Leadership Manual*, S. M. Bragg, Ed., Hoboken, NJ, USA: John Wiley & Sons, Inc, 2010, pp. 263–287.
[17] J. H. Block, M. G. Colombo, D. J. Cumming, and S. Vismara, "New Players in Entrepreneurial Finance and Why They Are There," *Small Bus Econ*, vol. 50, no. 2, pp. 239–250, 2018.
[18] J. A. Fehrer and S. Nenonen, "Crowdfunding networks: Structure, dynamics and critical capabilities," *Industrial Marketing Management*, 2019.
[19] P. Belleflamme, T. Lambert, and A. Schwienbacher, "Crowdfunding: Tapping the right crowd," *Journal of Business Venturing*, vol. 29, no. 5, pp. 585–609, 2014.
[20] P. Roma, A. Messeni Petruzzelli, and G. Perrone, "From the Crowd to the Market: The Role of Reward-Based Crowdfunding Performance in Attracting Professional Investors," *Research Policy*, vol. 46, no. 9, pp. 1606–1628, 2017.
[21] L. Hornuf and A. Schwienbacher, "Internet-Based Entrepreneurial Finance: Lessons from Germany," *California Management Review*, vol. 60, no. 2, pp. 150–175, 2018.
[22] R. Alt, R. Beck, and M. T. Smits, "FinTech and the Transformation of the Financial Industry," *Electron Markets*, vol. 28, no. 3, pp. 235–243, 2018.
[23] T. F. Dapp, "Fintech: The Digital Transformation in the Financial Sector," in *CSR, Sustainability, Ethics & Governance, Sustainability in a Digital World*, T. Osburg and C. Lohrmann, Eds., Cham: Springer International Publishing, 2017, pp. 189–199.
[24] I. Lee and Y. J. Shin, "Fintech: Ecosystem, Business Models, Investment Decisions, and Challenges," *Business Horizons*, vol. 61, no. 1, pp. 35–46, 2018.
[25] P. Gomber, R. J. Kauffman, C. Parker, and B. W. Weber, "On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services," *Journal of Management Information Systems*, vol. 35, no. 1, pp. 220–265, 2018.
[26] S. Underwood, "Blockchain Beyond Bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.
[27] C. Neagle, "Crazy Theories and Global Manhunts for Bitcoin's Creator Satoshi Nakamoto," (English), *Network World (Online),*

https://search-proquest-com.ezproxy.lib.swin.edu.au/docview/1505310679?accountid=14205, 2014.
[28] M. Swan, *Blockchain: Blueprint for a New Economy*. [Sebastopol, Calif.]: O'Reilly, 2015.
[29] N. Rao, "The Time is Now," (English), *Quality Progress*, vol. 51, no. 10, pp. 18–23, https://search-proquest-com.ezproxy.lib.swin.edu.au/docview/2131177148?accountid=14205, 2018.
[30] N. Hackius and M. Petersen, "Blockchain in Logistics and Supply Chain : Trick or Treat?," 2017.
[31] Freepik, *Locked Free Icon.* [Online] Available: https://www.flaticon.com/free-icon/locked_1590798. Accessed on: Mar. 30 2019.
[32] Freepik, *Blockchain Free Icon.* [Online] Available: https://www.flaticon.com/free-icon/blockchain_1594483. Accessed on: Mar. 30 2019.
[33] M. Milutinović, "Cryptocurrency," *Ekonomika*, vol. 64, no. 1, pp. 105–122, 2018.
[34] G. P. Dwyer, "The Economics of Bitcoin and Similar Private Digital Currencies," *Journal of Financial Stability*, vol. 17, pp. 81–91, 2015.
[35] L. P. Nian and D. L. K. Chuen, "Introduction to Bitcoin," in *Handbook of Digital Currency*: Elsevier, 2015, pp. 5–30.
[36] D. Yermack, "Is Bitcoin a Real Currency? An Economic Appraisal," in *Handbook of Digital Currency*: Elsevier, 2015, pp. 31–43.
[37] J. Surowiecki, "Cryptocurrency," (English), *Technology review*, vol. 114, no. 5, pp. 106–107, https://search-proquest-com.ezproxy.lib.swin.edu.au/docview/928060920?accountid=14205, 2011.
[38] F. Hartmann, X. Wang, and M. I. Lunesu, "Evaluation of Initial Cryptoasset Offerings: the State of the Practice," in *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, Campobasso, Mar. 2018 - Mar. 2018, pp. 33–39.
[39] S. Blemus, "Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide," *Revue Trimestrielle de Droit Financier (Corporate Finance and Capital Markets Law Review) RTDF*, no. 4-2017, 2017.
[40] M. Bacina, S. Kassra, and others, "Banking and Technology Law: Asic Guidance on Crypto-Currency Token Sales: A ban or Sensible Regulation?," *LSJ: Law Society of NSW Journal*, no. 39, pp. 86–87, 2017.

[41] W. A. Kaal and M. Dell'Erba, "Initial Coin Offerings: Emerging Practices, Risk Factors, and Red Flags," *Verlag CH Beck (2018)*, pp. 17–18, 2017.
[42] N. Lipusch, "Initial Coin Offerings A Paradigm Shift in Funding Disruptive Innovation," *SSRN Journal*, 2018.
[43] A. Collomb, P. de Filippi, and K. Sok, "From IPOs to ICOs: The Impact of Blockchain Technology on Financial Regulation," *SSRN Journal*, 2018.
[44] J. Li and W. Mann, "Initial Coin Offering and Platform Building," *SSRN Journal*, 2018.
[45] S. Lahajnar and A. Rožanec, "Initial Coin Offering (ICO) Evaluation Model," *Investment Management and Financial Innovations*, vol. 15, no. 4, pp. 169–182, 2018.
[46] L. Arnold *et al.,* "Blockchain and Initial Coin Offerings: Blockchain's Implications for Crowdfunding," in *Business Transformation through Blockchain*, H. Treiblmaier and R. Beck, Eds., Cham: Springer International Publishing, 2019, pp. 233–272.
[47] A. M. Antonopoulos and G. Wood, *Mastering Ethereum: Building smart contracts and DApps*. Sebastopol, CA: O'Reilly Media, Inc, 2019.
[48] T. Mathis, *Ethereum: Your Guide To Understanding Ethereum, Blockchain, and Cryptocurrency*: CreateSpace Independent Publishing Platform, 2018.
[49] A. Savelyev, "Contract Law 2.0: 'Smart' Contracts as the Beginning of the End of Classic Contract Law," *Information & Communications Technology Law*, vol. 26, no. 2, pp. 116–134, 2017.
[50] K. Timmerman and M. Thomas, "Ethereum: More than 'the new Bitcoin'," (eng), *Proctor, The*, vol. 37, no. 5, pp. 26–27, 2017.
[51] K. Roose, *Is There a Cryptocurrency Bubble? Just Ask Doge.* [Online] Available: https://www.nytimes.com/2017/09/15/business/cryptocurrency-bubble-doge.html. Accessed on: Mar. 19 2019.
[52] M. Wright and P. Desbrières, "Entrepreneurial Finance," in *Handbook of Research on Entrepreneurship*, A. Fayolle, Ed.: Edward Elgar Publishing, 2014, pp. 281–304.
[53] D. Boreiko and N. K. Sahdev, "To ICO or not to ICO – Empirical analysis of Initial Coin Offerings and Token Sales," *SSRN Journal*, 2018.
[54] M. Pilkington, "The Emerging ICO Landscape - Some Financial and Regulatory Standpoints," *SSRN Journal*, 2018.

[55] M. Adham, *The Ongoing Evolution Of The ICO*. [Online] Available: https://www.forbes.com/sites/forbesfinancecouncil/2018/11/27/the-ongoing-evolution-of-the-ico/#1f1076034516. Accessed on: Mar. 30 2019.

[56] E. Paulet, "Banking Liquidity Regulation: Impact on their Business Model and on Entrepreneurial Finance in Europe," *Strategic Change*, vol. 27, no. 4, pp. 339–350, 2018.

[57] W. Duggan, *Today In Cryptocurrency: EOS ICO Raises 4 Billion, Wikipedia Founder Calls Cryptos 'Absolutely, Definitely' A Bubble* (English), *Benzinga Newswires*. Available: https://search-proquest-com.ezproxy.lib.swin.edu.au/docview/2046166238?accountid=14205.

[58] K. Rooney, *A Blockchain Start-up Just Raised $4 Billion Without a Live Product*. [Online] Available: https://www.cnbc.com/2018/05/31/a-blockchain-start-up-just-raised-4-billion-without-a-live-product.html. Accessed on: Mar. 30 2019.

[59] H. E. Benedetti and L. Kostovetsky, "Digital Tulips? Returns to Investors in Initial Coin Offerings," *SSRN Journal*, 2018.

[60] M. Dell'Erba, "Initial Coin Offerings: The Response of Regulatory Authorities," (English), *New York University Journal of Law & Business*, vol. 14, no. 3, 2018.

[61] D. Lee and L. Low, *Inclusive Fintech: Blockchain, Cryptocurrency and ICO*. Hackensack, NJ: World Scientific Publishing Co. Pte. Ltd, 2018.

[62] B. Feld and J. Mendelson, "Crowdfunding," in *Venture Deals*, B. Feld and J. Mendelson, Eds., Hoboken, NJ, USA: John Wiley & Sons, Inc, 2016, pp. 123–128.

[63] C. Fisch, "Initial Coin Offerings (ICOs) to Finance New Ventures," *Journal of Business Venturing*, vol. 34, no. 1, pp. 1–22, 2019.

[64] D. Diemers, H. Arslanian, G. McNamara, G. Dobrauz, and L. Wohlgemuth, *Initial Coin Offerings: A Strategic Perspective*. [Online] Available: https://cryptovalley.swiss/wp-content/uploads/20180628_PwC-S-CVA-ICO-Report_EN.pdf. Accessed on: Mar. 19 2019.

[65] PwC, *Introduction to Token Sales (ICO) Best Practices*. [Online] Available: https://www.pwchk.com/en/financial-services/publications/introduction-to-token-sales-ico-best-practices.pdf. Accessed on: Mar. 19 2019.

[66] I. Simpson, *4th ICO and STO Report – growing less, but growing up*. [Online] Available: https://cryptovalley.swiss/4th-ico-and-sto-report-growing-less-but-growing-up/. Accessed on: Mar. 19 2019.

[67] C. Bovaird, *Is The ICO Market Truly Dead?* [Online] Available: https://www.forbes.com/sites/cbovaird/2019/01/16/is-the-ico-market-truly-dead/#5c7d0724536d. Accessed on: Mar. 19 2019.

[68] Ernst and Young, *EY study: Initial Coin Offerings (ICOs): The Class of 2017 – one year later.* [Online] Available: https://www.ey.com/Publication/vwLUAssets/ey-study-ico-research/$FILE/ey-study-ico-research.pdf. Accessed on: Mar. 12 2019.

[69] O. Kharif, *Crypto Coin Sales Stage Revival After Bursting of ICO Bubble.* [Online] Available: https://www.bloomberg.com/news/articles/2019-04-10/crypto-coin-sales-stage-revival-after-bursting-of-ico-bubble. Accessed on: May 02 2019.

[70] E. J. Schwarz, *Umweltorientierte technologische Prozeßinnovationen*. Wiesbaden: Gabler Verlag, 2013.

[71] B. Hotz-Hart and A. Rohner, "Neuerungen in der Wirtschaft: Das Konzept „Innovation", wirtschaftliche Dynamik und Innovationsprozesse in Netzwerken," in *Nationen im Innovationswettlauf*, B. Hotz-Hart and A. Rohner, Eds., Wiesbaden: Springer Fachmedien Wiesbaden, 2014, pp. 25–46.

[72] Coindesk, *Coindesk ICO Tracker.* [Online] Available: https://www.coindesk.com/ico-tracker. Accessed on: Mar. 13 2019.

[73] J. A. Cox and M. W. Rasmussen, Eds., *Blockchain for Business Lawyers*. Chicago, Illinois: ABA Section of Science & Technology Law, 2018.

[74] G. Fridgen, F. Regner, A. Schweizer, and N. Urbach, "Don't Slip on the Initial Coin Offering (ICO) - A Taxonomy for a Blockchain-enabled Form of Crowdfunding," in Portsmouth, 2018.

[75] M. Chanson, J. Gjoen, M. Risius, and F. Wortmann, "Initial Coin Offerings (ICOs): The Role of Social Media for Organizational Legitimacy and Underpricing," San Francisco, 2018.

[76] S. T. Howell, M. Niessner, and D. Yermack, "Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales: NBER Working Paper No. 24774," National Bureau of Economic Research, 2018.

[77] US Securities and Exchange Commission, *Spotlight on Initial Coin Offerings (ICOs).* [Online] Available: https://www.sec.gov/ICO. Accessed on: May 02 2019.

[78] Becris, *Transfer Free Icon.* [Online] Available: https://www.flaticon.com/free-icon/transfer_876784. Accessed on: Mar. 30 2019.

[79] Eucalyp, *Planning Free Icon.* [Online] Available: https://www.flaticon.com/free-icon/planning_1286803.

Accessed on: Mar. 30 2019.
[80] Freepik, *Networking Free Icon.* [Online] Available: https://www.flaticon.com/free-icon/networking_1333321. Accessed on: Mar. 30 2019.
[81] Itim2101, *Contract Free Icon.* [Online] Available: https://www.flaticon.com/free-icon/contract_1213707. Accessed on: Mar. 30 2019.
[82] G. Fenu, L. Marchesi, M. Marchesi, and R. Tonelli, "The ICO Phenomenon and its Relationships with Ethereum Smart Contract Environment," in *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, Campobasso, Mar. 2018 - Mar. 2018, pp. 26–32.
[83] T. Zalan, "Born global on blockchain," (English), *Review of International Business and Strategy*, vol. 28, no. 1, pp. 19–34, https://search-proquest-com.ezproxy.lib.swin.edu.au/docview/2011330670?accountid=14205, 2018.
[84] Ernst and Young, *EY study: Initial Coin Offerings (ICOs).* [Online] Available: https://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf. Accessed on: Mar. 12 2019.
[85] P. Gupta and T. M. Tham, *Fintech: The new DNA of financial services*. Boston: Walter de Gruyter Inc, 2019.
[86] J. Clayton, *Statement on Cryptocurrencies and Initial Coin Offerings.* [Online] Available: https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11. Accessed on: Mar. 17 2019.
[87] R. Keidar and S. Blemus, "Cryptocurrencies and Market Abuse Risks: It's Time for Self-Regulation," *SSRN Journal*, 2018.
[88] D. A. Zetzsche, R. P. Buckley, D. W. Arner, and L. Föhr, "The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators," *University of Luxembourg Law Working Paper*, no. 11, pp. 17–83, 2017.
[89] C. Feng, N. Li, B. Lu, M. H. Wong, and M. Zhang, "Initial Coin Offerings, Blockchain Technology, and White Paper Disclosures," *Mingyue, Initial Coin Offerings, Blockchain Technology, and White Paper Disclosures (September 25, 2018)*, 2018.
[90] P. Maume and M. Fromberger, "Regulations of Initial Coin Offerings: Reconciling US and EU Securities Laws," *Chicago Journal of International Law*, vol. 19, pp. 548–585, 2019.
[91] T. Scher, *ICOs and Appcoins: A Blockchain VC's View.* [Online] Available: https://www.coindesk.com/icos-appcoins-blockchain-vcs-view. Accessed on: Mar. 17 2019.

[92] I. M. Barsan, "Legal Challenges of Initial Coin Offerings (ICO)," *Revue Trimestrielle de Droit Financier (RTDF)*, no. 3, pp. 54–65, 2017.

[93] J. Eyers, *Regulatory regime for initial coin offering on the cards.* [Online] Available: https://www.afr.com/technology/regulatory-regime-for-initial-coin-offering-on-the-cards-20190315-h1cfjc. Accessed on: Mar. 31 2019.

[94] R. Amsden and D. Schweizer, "Are Blockchain Crowdsales the New 'Gold Rush'? Success Determinants of Initial Coin Offerings," *SSRN Journal*, 2018.

[95] D. B. Audretsch, N. Seitz, and K. M. Rouch, "Tolerance and Innovation: the Role of Institutional and Social Trust," *Eurasian Bus Rev*, vol. 8, no. 1, pp. 71–92, 2018.

[96] Pinsent Masons, *Bitcoin, Blockchain & Initial Coin Offerings: A Global Review.* [Online] Available: https://www.pinsentmasons.com/PDF/2017/FinTech/Bitcoin-Blockchain-guide.pdf. Accessed on: Mar. 17 2019.

[97] The Australian Government the Treasury, *Initial Coin Offerings: Issues Paper.* [Online] Available: https://treasury.gov.au/sites/default/files/2019-03/c2019-t353604-Issues_Paper-1.docx. Accessed on: Mar. 26 2019.

[98] J. Clayton, *SEC Rulemaking Over the Past Year, the Road Ahead and Challenges Posed by Brexit, LIBOR Transition and Cybersecurity Risks*. [Online] Available: https://www.sec.gov/news/speech/speech-clayton-120618#_ftn1. Accessed on: May 02 2019.

[99] W. Huang, M. Meoli, and S. Vismara, "The Geography of Initial Coin Offerings," *Small Bus Econ*, vol. 40, no. 1, pp. 1–26, 2018.

[100] C. Catalini and J. S. Gans, "Initial Coin Offerings and the Value of Crypto Tokens: NBER Working Paper No. 24418," National Bureau of Economic Research, 2018.

[101] S. Adhami, G. Giudici, and S. Martinazzi, "Why do Businesses go Crypto? An Empirical Analysis of Initial Coin Offerings," *Journal of Economics and Business*, vol. 100, pp. 64–75, 2018.

Authors Biography

Dimitrios Salampasis (PhD) is the Director, Master of Financial Technologies (MFinTech), Financial Technologies Innovation Program Leader at the Swinburne Data Science Research Institute, and Lecturer of Entrepreneurship and Innovation at the Swinburne Business School, Swinburne University of Technology in Australia. Prior to joining

academia, Dimitrios worked in the management consulting industry, being involved in global advisory and consulting activities on investing in emerging markets, and assisting companies in developing long-term strategic focus and sustainable market business strategies. Dimitrios has published in international peer-reviewed academic and practitioner journals and books, and his work has been presented at major international conferences and invited keynote speeches and lectures around the world.

Mark Pickering (PhD) is an Associate Professor in the accounting, economics and finance department at Swinburne Business School. Mark was the inaugural Director of the Master of FinTech at the Australian Graduate School of Entrepreneurship at Swinburne University of Technology in Australia. Prior to joining academia, Mark worked in the accounting and management consulting industries for over 20 years, including as a partner in one of the 'Big Four' accounting firms. Mark has consulted with companies in the banking, manufacturing, and telecommunications industries, in areas such as strategic planning, operational effectiveness, organizational design, business case development, and analysis of product and customer profitability. Mark's research has been published in respected journals, such as *Organization Studies* and the *Journal of Organizational Behavior*.

Volkmar Klaußer (MSc) is a Test Manager at Finanz Informatik Solutions Plus GmbH. Volkmar has more than seven years of professional working experience in entrepreneurial teams in the financial services industry. Volkmar is responsible for the development of a test environment for apps, and manages IT-projects as a sub-project lead. Volkmar has previously completed his studies in technology and innovation management at the FOM University of Applied Sciences for Economics and Management, writing a Master's thesis on the '*Development of a Smart Lending Process for Private Customers in Germany*'. Currently completing his Master's in Business Administration (Executive) and Entrepreneurship and Innovation at the Swinburne University of Technology in Australia, Volkmar's research is focused on how emerging technologies can improve the services provided by the financial industry.

CHAPTER EIGHT

AI-ENABLED IOT NETWORK IN THE AGRICULTURAL FOOD CHAIN USING BLOCKCHAIN TECHNOLOGY

MD. MONWAR JAHAN CHOWDHURY[1], MONIRUL ISLAM PAVEL[2] AND SAIFUR RAHMAN SABUJ[1]

[1]Department of Electrical and Electronic Engineering, BRAC University, Bangladesh
[2]Department of Computer Science and Engineering, BRAC University, Bangladesh

Abstract

There is an increasing number of internet of things (IoT) devices connected around us, for various purposes, including healthcare, agriculture and military. As the IoT is creating a large volume of data, security of data has become a major concern, due to the increasing risk of cyber-attacks. Blockchain, which is a distributed, tamper-proof ledger, can be considered a smart security solution for IoT devices. As it is decentralized and distributed, security of information is more reliable. In developing countries, such as Bangladesh, a selling price to customers can be almost eight times higher than the buying price from farmers, and as a result, both consumers and producers are facing financial problems. This paper proposes a blockchain-based, IoT-supported agriculture model, aiming to track the distribution of agricultural goods from producers to consumers, in order to reduce discrimination and ensure quality. IoT devices collect the primary data, for example, the amount of crop production, the pH and moisture of land, air quality, land condition, and distribution tracking. Then blockchain blocks are created using the BigChain database, and dApp and Hyperledger Sawtooth platforms. This

contains the price of crops and other necessary information, with external information, such as market demands, equilibrium price, amount, and distribution, based on the population of urban and rural places. Then the XGBoost algorithm-based prediction model is developed to make an artificially intelligent suggesting system, to increase agricultural productions based on primary field data acquired from the embedded device, with 98.78% accuracy. The proposed model ensures transparency in the whole system, product price balancing, economical sustainability, and securing of the decentralized data in each category of this process.

Keywords: Blockchain, Hyperledger Sawtooth, XGBoost, internet of things, BigChain database, embedded system, agricultural sensing, Node MCU, blockchain for agriculture, prediction system.

1. Introduction

The internet of things (IoT) is a major breakthrough innovation that is redefining the usability of the internet. The IoT can be defined as a network of smart devices, sensors, and actuators that are connected with each other, and the surrounding environment, to continuously send and receive data for various purposes. [3] The application of the IoT can be extended from home to healthcare, agriculture to military industry, automation, etc. As IoT devices are continuously connected to the internet, creating a large amount of data for processing, security concerns have become a major issue. IoT devices are becoming more vulnerable to cyber-attacks and security risks day-by-day. In 2016, the IoT Botnet attack caused internet disruption to millions of users, as well as financial losses. Organizations are now spending more money to keep their data safe from threats and tampering. It has been predicted that 547 million US dollars will be spent globally in 2018 to protect IoT devices from threats. [1] Most of the current IoT solutions depend largely on huge centralized cloud architecture, which involves security threats such as data tampering, data corruption, and issues of confidentiality and auditability. Blockchain, which has recently attracted the attention of researchers, can be an important tool to tackle IoT security concerns. Blockchain can be referred to as a chain of blocks of data that enables the creation of an alteration-proof distributed ledger in a peer-to-peer network. [4] Blockchain offers greater security and transparency in financial transaction activity, anywhere. As every transaction is secured with a time stamp, and a majority stakeholder decision is needed to change any information in the block, it provides greater security than conventional online banking

systems. Blockchain ensures traceability, efficiency, and cost minimization in any kind of business, because in this system, information is maintained in a distributed ledger. People can see how the transaction is going, from where it started, and middle parties can also be eliminated. Due to all these benefits, people have started to use blockchain applications for financial transactions, agriculture supply chain modelling, industry optimization, etc.

Researchers and scientists all over the world are now focused on building a blockchain-based supply chain model of agricultural products for various purposes, as the conventional supply chain systems in food and agro businesses have failed drastically to provide traceability, accountability and fair pricing for farmers who are at the very low stages of the existing supply chain model. Farmers get very poor prices for their crops through existing models, as there are lots of steps from production to consumer consumption. They are deprived of fair prices for their crops, due to middlemen in the system. The existing supply chain model, which consists of farmers as producers, suppliers, retailers, distributers, regulators, and consumers, is yet to maintain proper strict guidelines for produced crops. According to a survey conducted by IBM, every year, 600 million people fall ill after eating contaminated foods, and 420,000 people die among them. The total cost of foodborne illness alone in the US in 2018 is 93.2 billion USD, which is 4% higher than in the previous year. [2] So, food safety has become a vital concern for government, as huge amounts of money and resources are wasted every year due to this. A blockchain-based agro model can be a good solution to food safety concerns, because in a blockchain model, people can very easily identify the materials present in the foods, and whether food is contaminated or not, within a couple of seconds. Secondly, farmers can hugely benefit from blockchain-based supply chain applications. When crops are ready for sale in the market, with the help of blockchain-secured blocks, governments will assign fixed price for their products, and they can sell it directly in the desired centers, built by government, removing the middleman syndicate. With the advancement of AI and the IoT, blockchain will replace the existing agro supply chain model with a more advanced and efficient supply chain model which will benefit both consumer and farmer, in every aspect.

The main contribution of this chapter is that we introduce an AI-enabled smart supply chain model for agriculture, based on IoT and blockchain, to provide food security, transparency, and scalability monitoring for all. With the help of IoT devices, various parameters like temperature, air pH,

and soil humidity, which are related to the agro supply chain, will be collected, and after processing, classified data will be stored in blockchain. We used an XGBoost algorithm for the prediction of crop production, weather reports, and farming land conditions. To study the feasibility of the proposed solution, the model is tested on two platforms, i.e. Hyperledger Sawtooth and Ethereum, for measuring latency, CPU load, and memory usage. Finally, the accuracy performance of different prediction systems is analyzed here, and XGBoost shows superior performance comparison to other models.

The rest of the chapter is organized as follows. Section 2 contains a brief literature review of blockchain and IoT in the agro supply chain. Section 3 presents an overview of the topic, and introduces a system model of a smart food chain. Details of the implementation technique are also discussed here. Section 4 analyzes the performance metric of the system, with numerical analysis of various prediction systems. Section 5 concludes the paper with the findings of this study.

2. Literature Review

Caro et al. presented a traceability system for agri-food supply chain management systems based on blockchain, to avoid unsolved problems of IoT based agri-food supply chain management, such as data integrity, tampering, and single points of failure. They proposed the decentralized blockchain-based traceability solution 'AgriBlockIoT', which is capable of seamless integration of IoT devices and digital consumption data along the chain, and where traceability is obtained applying two different blockchain implementations, named Ethereum and Hyperledger Sawtooth. Latency, CPU, and network usages are compared, and their main pros and cons are highlighted. [1]

The security issues and challenges in the IoT for blockchain technology have been shown by Kumar et al., where the concerns of security and privacy of the IoT, when exchange of information and data authentication is only done through the central server, are presented. The main purpose of their research was to show the distributed ledger-based blockchain (DL-BC) as a part of IoT, and its application to prevent device spoofing, and false authentication. [4]

Tian briefly described a system of food safety in the supply chain implementing the IoT, blockchain, and HACCP (hazard analysis and critical control points). The trust issues of fraud, tampering corruption, and

wrong information may be contained in the development of the IoT-based supply chain system. Moreover, in being centralized, if one single point breaks down, all data can be corrupted, or the system can be crushed. Focusing on decentralization and HACCP, a real-time food supply chain traceability system can give a data stage for all the supply chain individuals, with openness, straightforwardness, lack of bias, reliability, and security. [5]

Dinh et al. showed a data processing view of blockchain systems, and a benchmarking framework named 'BLOCKBENCH' to experience the performance of a private blockchain, where parties or agents are authorized along with data processing workloads. The research presented the design space and performance differences between database systems. [6]

A comprehensive survey of the protocols of blockchain for IoT networks is represented in the research of Ferrag et al., who began by describing the primary theory of blockchain, and existing surveys on blockchain technologies. Furthermore, applications of the IoT like the internet of vehicles, the internet of cloud, edge computing, and five properties of blockchain protocols in IoT networks, are described in their research work. Blockchain technologies, with respect to the blockchain model, specific security goals, performance, communication overhead, limitations, and computation complexity, are compared on security and privacy preserving. [7]

Liu et al. showed a solution for the drawback of blockchain's non-supervisability and computational overhead, by introducing NormChain, which is a blockchain-based IoT-enabled autonomous transaction settlement architecture, containing three layers. The authors presented a decentralized public key searchable encryption scheme to prevent illegal transactions and provide better traceability. Their proposed architecture achieved 100% accuracy in terms of supervision on target keywords during transactions, and scored around 113 transactions per second on IoT devices. [8]

The architecture of a double-chain-based public blockchain mechanism for the agricultural supply chain system is proposed by Leng et al. [9] The authors integrated their proposal with a consensus algorithm for data storing with intelligent contact, decentralized collective maintenance, matching mechanisms, and rent-seeking resource adaptive design, aiming to demonstrate the agricultural supply chain model. The research outputs

show the system of double-chain-based blockchain to solve the transaction information and secure openness of the account by maintaining privacy of the enterprise data. Additionally, the system is fully rent-seeking-enabled, along with information matching techniques.

3. Proposed Methodology

We propose an artificial intelligence-enabled system, implementing the IoT and blockchain, to improve the growth of agricultural products, predict environmental parameters, trace production to the hands of customers, and develop a better system for product supply, maintaining transparency in each step.

3.1 Internet of Things (IoT) with Blockchain

The general concept of the IoT is to connect multiple devices with internet access and control, from anywhere. Basically, it is media which optimizes and transforms manual processes into problem-solving in the digital era, along with the obtaining of huge amounts of data from any place. This is one of the most important elements in facilitating the development of intelligent appliances to enhance the quality of lives through digitalization of a city. In this decade, the interaction of cloud computing, edge computing and fog computing has contributed a great deal to improving the functionalities and applications of the IoT, in order to analyze, process information, and make it usable in real-time scenarios. [10] Along with these appliances, the new dimension of mechanisms to access and exchange information has contributed to the massive growth of the IoT in recent years. In spite of the unprecedented growth of IoT-enabled embedded systems and devices, the lack of confidence in security, and centralized focus issues have become serious concerns. Traditionally, or in general cases, centralized distributed architectures, like cloud-based systems, are used in interfacing the IoT, but it also has data transparency and security issues, where end users may have no clear understanding of how and where the obtained data from IoT-enabled devices are stored or will be used. As mentioned above, for any random IoT network, a crucial threat is raised by its scattered placement of nodes or devices. As there are huge number of nodes connected to the internet for continuous sharing and storing information, at any given point there lies the risk of vital cyber-attack, such as distributed denial of service, phishing, etc. If the majority of nodes are affected, an IoT network may collapse at any moment. In these worst-case scenarios, the confidentiality of users' personal data is

completely vulnerable. Without the presence of strong security features on an IoT network, user data can be very easily exploited. IoT devices are generating tons of data continuously; accuracy of these data needs to be very high. In real world applications, such as healthcare, smart grids need very high levels of accurate data for monitoring and supervision. So, it is important that, from generation of data to transmission to proper channels, data needs to be unaltered and protected from various types of SQL injection attacks. [11] Injection attacks provide the opportunity to inject wrong data into the network, making the whole database untrustworthy and corrupted. To mitigate all these security threats, and make the IoT network a bit more compact and secure, blockchain has come onto the scene, offering the network immunity from cyber threats. With a view to solving these issues, blockchain has great potential for revolutionizing the present architecture of the IoT by providing trusted and secure transactions and safe data exchange, as the information sharing always can be traceable. As it is a distributed, decentralized, and tamper-proof ledger, blockchain can be used in applications from financial transactions to the supply chains of larger automated industry. The application of blockchain in many industries is now booming, because of its transparency, cost minimization ability, increased efficiency and high protection from outside cyber-attacks. [12]

3.2 Hardware Setup and the Internet of Things, Implementing NodeMCU

In this research, we developed a NodeMCU based on two different devices implementing the IoT. One is for agri-farm monitoring, and the other is for distribution purposes. The NodeMCU, which is shown in Figure 1, is known as a wi-fi module with an IoT platform that has firmware based on ESP8266 -12E. It contains ten digital GPIOs, one analog GPIO, SPI and IIC communication, PWM functionality, PCB Antenna, 1-wire, USB TTL, [13] along with 32-bit RISC 160MHZ-based Tensilica L106 processor, 4MB SPI Flash, 36KB internal SRAM,[14] and can be programmed collaborating with Arduino IDE.

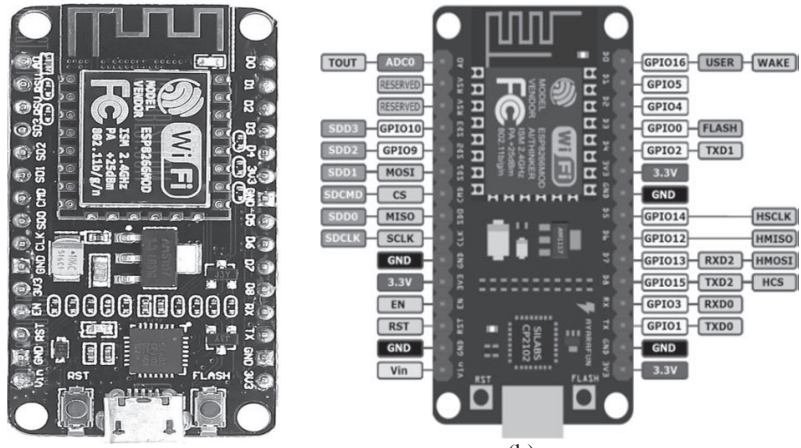


Figure 1. (a) ESP8266 based NodeMCU V2 [15], (b) pin diagram of NodeMCU [16]

In the first phase of the device setup, which is shown in Figure 2a, the primary goal is to make an agri-farm-based sensing device to monitor the farming land, analyzing the soil and air quality for better production. [17] In order to obtain the air temperature, DHT22 can sense temperature within a range of *-40□ to 80□*. [18] The same sensor is used to measure air humidity. Furthermore, the MQ135 gas sensor is implemented to measure the ppm values of ammonia (NH_3) and carbon dioxide (CO_2). [19] The grove oxygen (O_2) gas sensor is used for obtaining the percentage of oxygen in the air. The sensor is able to measure air sensibility ranging between *0.10 - 0.25 mA,* and volume up to *30%.*[20] We measure soil pH and soil moisture, to monitor the soil quality. A gravity analog pH meter [21] measures the pH level after wetting the soil sample. This sensor comes with a LED power inductor and a BNC connector which, combined, convert the analog voltage value into pH level. To detect soil moisture and continuous wetness, the grove moisture sensor is used.

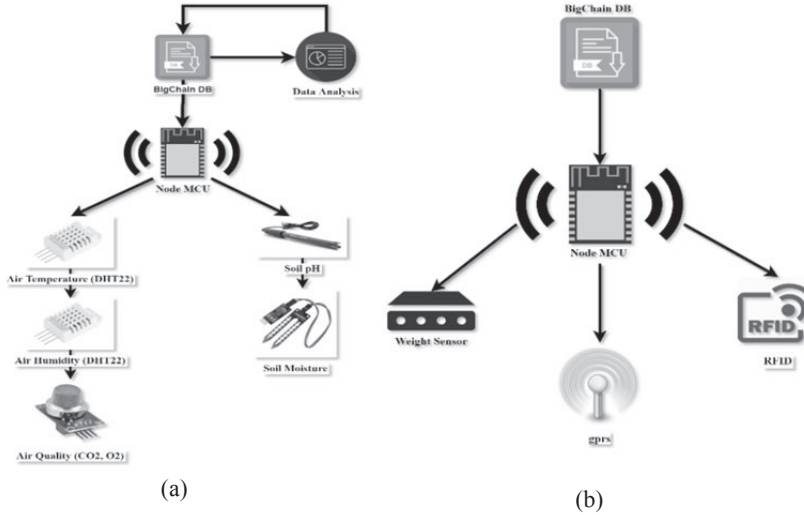


Figure 2. (a) Block diagram of phase 1, (b) Block diagram of phase 2

NodeMCU has only one analog pin, and, as all sensors without DHT 22 are analog sensors, an ADC (analog to digital converter) is connected to each analog sensor, to read their values. Here, ADC0804 is applied as the converter, which takes *100μs* for conversion, and the resolution is 8-bit. In the second phase, Figure 2b, the RFID (Radio Frequency Identification)-based tracing and tagging system with smart weight monitoring system is shown. The ID-12LA RFID reader and USB RFID reader are connected, and each tag or RFID-enabled 125 kHz card has unique 32-bit ID, and comes with FTDI chip.[22] For smart weight measurement, we proposed to use a 100kg load cell, interfacing with a HX711 load cell amplifier module. [23] Finally, for location monitoring, sim900A is used as the GPS module, to get longitude and latitude.

3.3 Building a Smart Supply Chain Model with IoT

The traditional supply chain model mainly focused on supply and distribution of goods and products, and is now undergoing a revolutionary change, due to the integration of the IoT, cloud, and blockchain in existing supply chain models. Integration of the IoT in supply chain models has greatly changed the idea of how products are produced, distributed, and finally supplied, to the end user or customer. In any random supply chain model used in agro-farming, industry, or military application, first of all,

planning is done to make sure that the right product, which will attract the attention of the customer, is made. Before going into production, huge research has to be done on cost management, source of profit, and efficient use of skilled manpower. The next stage includes collecting information, selecting sources and proper inventory management. In order to make the business run smoothly, multiple suppliers should be selected for raw material delivery, and ingredients need to be continuously monitored to ensure superior end commodity production. After that, the next step is producing the desired output, after successful completion of rigorous testing, and obtaining the permission of the regulatory standard bodies of respective countries. Quality compliance should be maintained at every step to ensure the safety of products. Finally, products are delivered to various places, via warehouse, inventory, and distributers. Selecting a proper transportation channel, and location of stores, are very crucial for a business to run and survive successfully in the long run. In order to ensure nominal loss and zero damage for goods and supply, transportation systems need to be very compact, and managed by experienced people. Another vital factor to run the business efficiently is proper location selection. Production units or factories should be located where ingredients can be provided conveniently, and distribution of material can be done effectively and efficiently. Organizations also need to provide warranty for products where applicable, and facilitate the return the defective products from distributers. Products which have reached their end-of-service life, meaning the company will not provide any servicing for them, also need to be returned from the market. The traditional supply chain model, as stated above, also has some serious drawbacks, such as absence of proper accountability or transparency, unpredictable pricing and demand-supply imbalances, high transportation costs, and lack of proper inventory management. [24] Like every other sector, such as smart home, and e-health, the IoT is now changing the way the existing supply chain model works, and replacing it with a smart model which is cloud feature-enabled, with proven efficiency. One of the biggest concerns in any business is tracking of goods and supply, and how to deliver the product to the end customer in the quickest and most efficient way. Business organizations are now investing huge funds in tracking goods and services. Tech giants DHL and Cisco observed that nearly 1.9 trillion US dollars will be spent on tracking solutions in the transportation domain of the supply chain model. [25] Another recent survey by GT Nexus and Capgemini stated that around 70% of production and manufacturing organizations have implemented various digital solutions in their supply chain systems. Smart RFID tagging and vehicle management systems are two examples of

internet-connected digital solutions available for the monitoring of transportation.[26] Managers can easily check the condition and location of their vehicles via their smartphones or web-based servers. As they are IoT-connected devices, they can be accessible from anywhere, and devices will send emergency signals to corresponding people if the vehicle faces a collision or an accident. In remote places, where there is minimal or zero internet facility available, vehicles can be tracked by GPS technology. Transparency and accountability can also be increased by implementing the IoT, as each transaction will be verified electronically online, with a secured payment gateway system. In the IoT, devices connected to the network will continuously transmit data and store them online for later use. Managers can easily access the data in the server, and analyze the current state of production. The AI-enabled IoT can predict each month's demand, and production managers can use the data to set the output for each specific product, for each specific region. A practical real-life example of the IoT in the supply chain is the UCOT IoT solution, which sends the information data from IoT sensors to a decentralized blockchain system which is more secure. [27] This device can also detect if the product is fake, or there has been alteration by an unauthorized person. Managers will receive a message on their mobile if the temperature of the inventory goes above the value set by this smart solution.

3.4 Communication and Process to Blockchain

All the data obtained from two devices are sent to a decentralized private MySql database, before transmitting to blockchain to apply a machine learning approach for prediction purposes. NodeMCU is inbuilt with wi-fi, and sends an http request after combining all the values of sensors, along with the domain, in a URL format. A backend program based on php language is created, which is connected with the database, and able to handle the http request. This program splits the URL, categorizes the columns of the database namewise, and posts it to the decentralized database. If any sensor loses connection or is damaged, it will send an unusual five digit 'fix' number, which will be a way to troubleshoot, monitoring the real time data.

Furthermore, the processed data, and data inserted from every step of the working diagram, are sent to build the blockchain via BigChain database [28] and Hyperledger Sawtooth. [29] [30] The BigChain database is widely used for storing information of blockchain. The chain service is called a Dapp (decentralized application) Frontend, along with the asset ID

of the BigchainDB to be processed by Hyperledger chaincode. [31] This chaincode, which has the functionality to call rest api, processes logics and rest api in oracle components. The rest api with oracle concatenates between BigChainDB and Hyperledger Sawtooth. Hyper Sawtooth is an enterprise-distributed ledger and open source blockchain platform. Consensuses, which are techniques to pick the leader of a new block, are the foundation of each blockchain stage, and Hyperledger Sawtooth gives three consensuses executions: Dev mode, PoET, and PoET Simulator, which uses proof of elapsed time (PoET), which depends on Intel's software guard extensions (SGX) and where the core theme is to get the waiting time of each node before they are allowed to be generated. SGX is implemented during creation of the node of the block, by generating and verifying a proof of the waiting time. [32] It is extremely scalable and is able to withstand high throughput of data, which makes it a great option for production supply chain scenarios, and comes with a lot of features, such as:

1. Shared: Blockchain does not contain any central data server in its system, so all the information is shared among all the active contacts. All blocks in the network contain the same information.
2. Unmodifiable: Once the information is stored in the blocks of the blockchain network, data cannot be changed or modified. Any attempt to modify the data will alert all the users of the network.
3. Protected: All the transactions that occur inside the blockchain network are verified by high level, trustworthy, contacts. In this way fraudulent activity can be minimized.
4. Flexible with permission infrastructure: Blockchain gives its users the option of permission, or permission less. Users who don't have access to enter the network can still use it for various purposes. Later, if they are verified by all other blocks, they can enter the network fully.
5. Simultaneous execution: Many transactions can be performed simultaneously in the blockchain network, thus increasing performance, and security for all.
6. Modular: It provides a stage for exchanging transaction-based updates to shared state (data) between untrusted parties.
7. Hardware coordination: In addition to certain open blockchain highlights, Hyperledger Sawtooth has turned out to be known for the simplicity with which it may be incorporated into equipment security arrangements. [33]

3.5 Implementation of Blockchain in the Field Process

The term was first introduced by Satoshi Nakamoto back in 2008, for use in digital currency, called bitcoin. [34] Since its innovation, the use of blockchain in financial transactions, smart homes, agriculture, and many more sectors, has increased rapidly. The most important advantage of blockchain is decentralization. Every block in blockchain has data encryption, secured time stamp, shared consensus algorithm, and other improved mechanisms, to keep it safe and secure. When two parties who do not fully trust each other agree on a transaction in blockchain, a new block is created. [6] Each new block has its hash, connected to the preceding block of blockchain. The transaction is sent to the entire network of peers connected to the blockchain. Nodes (people) connected to the network can then authenticate the transaction, and take steps to validate it. All the valid transactions are set inside a block, which is then sealed. Since any transaction in the blockchain needs to be authenticated by a large number of people in the network, it is nearly impossible to tamper with, or duplicate, any transaction without the consent of a vast number of people, which is unlikely to happen.

To address the existing agro-supply chain model problems discussed beforehand, [35-41] we propose a novel, blockchain-based, supply chain model. First, we provide security for foods by placing them in a unique block in the model. Next, farmers will get different time stamps for various crops they produce, which will contain the price, weight, sales commission, etc. In our supply chain model, AI will set the equilibrium price, product distribution, and market demand, based on the population of a specific region. Finally, in our distribution model, farmers will get a fair price for their crops, and consumers will benefit, as it ensures traceability, security, and sustainability for all. We will implement a private blockchain mechanism (Figure 3), as it has faster transaction times, known pre-approved end users, and multiparty consensus.

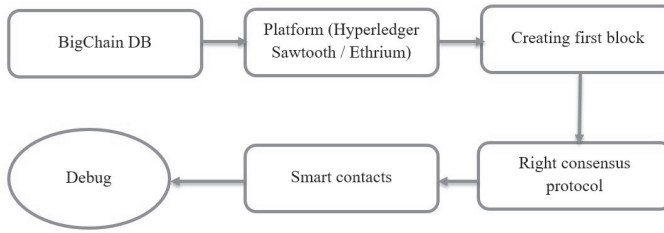


Figure 3. Blockchain implementation steps

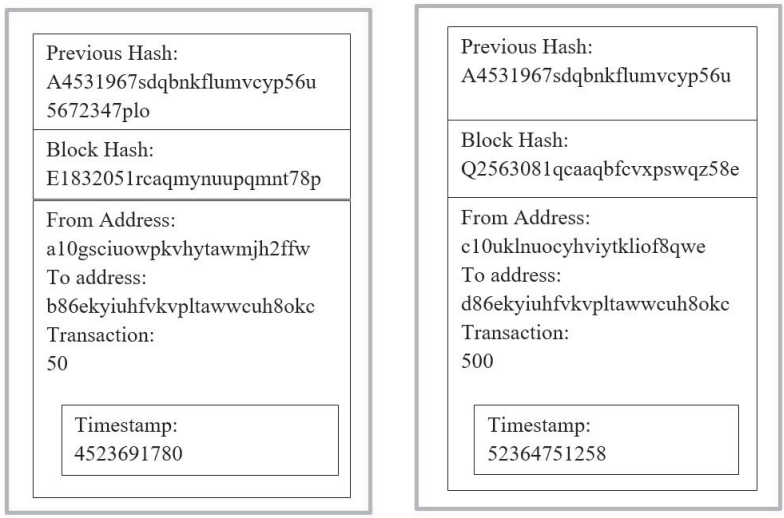


Figure 4. Sample blockchain transaction

The figure 4 is a sample transaction of Node A and Node B. When A wants to send something to B in blockchain, first a block is created containing the transaction data, which is validated by the majority of nodes of the network. With an interval of ten minutes, the whole transaction is put into a cryptographically sealed block. All blocks in the blockchain network are linked to former blocks, using hashing. Hashing refers to the process of taking any input of variable length and producing an output of fixed length. [42] The following example uses a hashing algorithm called SHA-25 (secure hashing algorithm), which always returns an output which consists of 25-bit. In SHA, a very slight change in input, such as adding a space or turning a small letter into a capital letter, will bring a radical change in the output. A very important characteristic of blockchain is that every blockchain has a linked list which stores data, and a hash pointer which consists of the address and hash data of former blocks. If anyone wants to change any information in any particular block of the network without validation, due to the hashing property, all blocks need to be updated in the system, which is nearly impossible. Hashing provides blockchain immutability, which is one of the core advantages of this network. In order to make sure everyone has the same ledger, blockchain uses the Merkle tree hashing method to verify the transactions, making the system efficient and low energy consuming. In our proposed system

model, we have used SHA-256-bit for advanced protection. [43] The fixed prices of the crops will be stored in blockchain blocks for further validation. Only approved authorities can add new blocks or modify the existing information in blocks. Consumers will benefit from this system, as information related to the products, such as price, weight, and expiry date, will be stored in the chain. They can verify the product within a couple of minutes, to check its authenticity.

In south Asian countries, such as Bangladesh and India, the prices of agricultural goods in the market get much higher than the farmers' selling costs, because of the lack of monitoring in the middle processes between the farmers and the market. As a result, price equilibrium can't be maintained by the government. To solve this problem, our proposed system can be a media for the development of agricultural economics. This whole process runs through an android application or web interface, which needs to be very user-friendly and easy-to-use for every end-to-end user, focusing on all farmers, suppliers, and field agriculture officers. Each role has a certified account from government, and no one else can edit once the data is uploaded. Figure 5 shows the total role in each step, as described below:

1. Purchasing raw materials: When governments or producers are purchasing raw materials like seeds, or fertilizers, information about the amounts and prices is stored in blockchain, with QR codes for further tracing.
2. Planning based on AI suggester: All the predicted environmental parameters are stored in blockchain and shown in the user interfaces of producers, farmers, and field workers, so that they can take necessary steps towards better production.
3. Field planting process: Farmers or producers record their planting information in blockchain. The amount and weights they use for their lands are stored, and as a result, transparency is created if a registered farmer or producer uses less material than they have given, or used more fertilizers compared to their maximum limit. Moreover, if sensors note values which cross thresholds, automatic alerts are sent to relevant people.
4. Harvesting and primary packaging: Farmers have to come into their nearest union's harvesting scaling zone, where they measure the weights of their products, using the proposed smart machine, after successfully logging in. The data of each farmer's harvesting, along with farming information, RFID tags containing all related data, and prices set by government, are all sent to be contained in the

blockchain. The agricultural zone officers also mark harvesting quality, by leveling the products, so that retailers and customers can get their desired products.

5. Transportation tracking: Locations, transportation information, starting times, current locations passed, and arrival times are stored. Any hassle in reaching destinations can be marked, so that transparency in highway transport is ensured, which is very important in south Asian countries.
6. Process to packaging: Information about packaging detail, including the amount obtained from distributors, the packaged weight, the status of the product and finally the total loss of product compared with the amount received, is stored in blockchain.
7. Delivery to suppliers: The process of ownership handover, amount paid, and distribution plans, are recorded in blockchain, based on scanning the RFID tags and QR codes of packaged products.
8. Suppliers to stores: Product information, such as price, weight, expiry date, and previous origin of products, are stored in blockchain through this character. The system shows warnings when the batches are near to their expiry date.
9. Consumers: Customers can easily verify the history, status, location, and all the processes a product has passed through. This is done by the smart tagging system of the product.

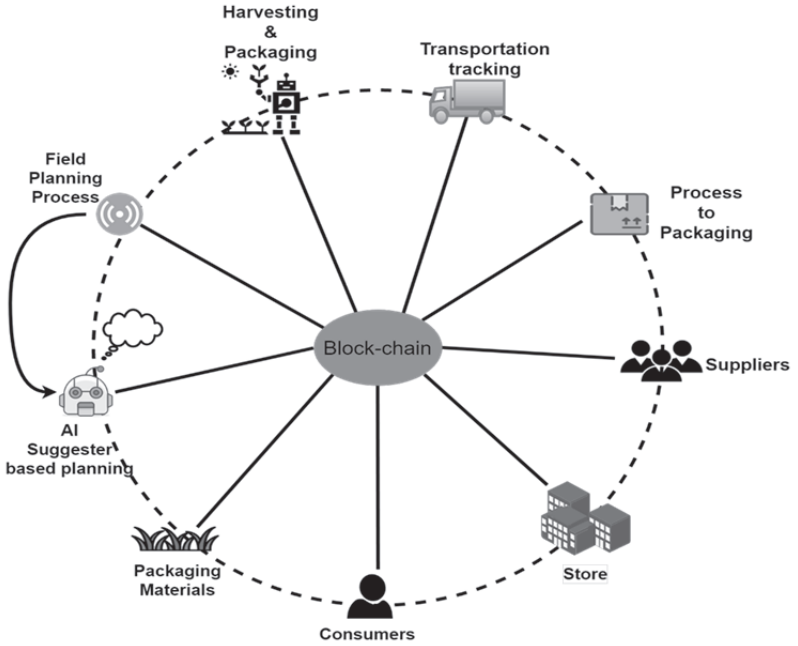


Figure 5. Blockchain implementation in proposed model.

3.6 AI Suggester and Prediction System

This aims to build an 'auto suggester', based on artificial intelligence, which predicts the farming land conditions, forecasts weather by obtaining the primary data from our device, predicts population growth for perfect distribution, and marks price equilibrium points based on the dataset of the World Bank,[44] where data from 1960 to 2017 are available. We applied an XGBoost (Extreme Gradient Boosting) algorithm for this prediction model. [45-50] XGBoost is an optimized version of Gradient Boosting Decision Tree (GBDT). The core function of GBDT relies on many decision trees, rather than a single one. The benefit of this theorem is that many decision trees can give odd results, but integrating all of these gives better performance and good accuracy. XGBoost has been developed mainly to solve supervised learning problems, where it denotes the mathematical structure which is applied to obtain the future value of b_i after training data with multiple features of a_i. To develop the prediction model, firstly, we pre-processed the dataset. In this phase, errors and

dissimilar values are removed to reduce the error. We check the next, and previous five minute, values, and average those to fill the empty values of parameters. Moreover, we set a long value if any sensor node is disconnected, and further fetching of those values is removed. Afterwards, the dataset is divided into training and testing parts. The training model finds the best possible fit parameters θ of training data a_i and model b_i. An objective function is declared, which is a combination of training loss and regularization, to verify how well the model is fitting in the training dataset. Here, in Equation 1, regularization *R(θ)* shrinks the coefficient approximation towards zero to prevent the risk of over fitting. Training loss *L(θ),* which refers to mean square error, measures the accuracy of prediction along with the training and testing dataset.

$$\mathrm{obj}(\theta) = \mathrm{L}(\theta) + \mathrm{R}(\theta) \tag{1}$$

Generally, the free ensemble model has a set of classification and regression trees, shortly CART. If k denotes the total number of trees, F refers to the set of all CARTs and f is mentioned as the function space of F:

$$\mathrm{obj}(\theta) = \sum_i^n L\left(b_i, \hat{b}_i\right) + \sum_{k=1}^k R(f_k) \tag{2}$$

To train the training dataset using XGBoost, we need an objective function which is shown in Equation 2 and we need to optimize it. As learning tree architecture is more complex than traditional optimization, where gradient can be easily taken, we can use additive strategy where the complexity can be reduced by adding new trees one by one, instead of all trees at once. If the prediction value at step q is $\hat{b}_i^{(q)}$,

$$\left.\begin{aligned}
\hat{b}_i^{(0)} &= 0 \\
\hat{b}_i^{(1)} &= f_1(a_i) = \hat{b}_i^{(0)} + f_1(a_i) \\
\hat{b}_i^{(2)} &= f_1(a_i) + f_2(a_i) = \hat{b}_i^{(1)} + f_2(a_i) \\
\hat{b}_i^{(3)} &= f_1(a_i) + f_2(a_i) + f_3(a_i) = \hat{b}_i^{(2)} + f_3(a_i) \\
&\ldots\ldots\ldots\ldots \\
&\ldots\ldots\ldots\ldots \\
\hat{b}_i^{(q)} &= \sum_{k=1}^q f_k(a_i) = \hat{b}_i^{(q-1)} + f_q(a_i)
\end{aligned}\right\} \tag{3}$$

Now, from Equation 2, to get the tree which is needed to optimize for our objective, the following equation is developed as:

$$obj^{(q)} = \sum_{i=1}^{n} L(b_i - \hat{b}_i^{(q)} + \sum_{i=1}^{q} R(f_i)$$

$$= \sum_{i=1}^{n} L\left((b_i - \hat{b}_i^{(q-1)}) f_q(a_i)\right) + \sum_{i=1}^{q} R(f_q) + constant \tag{4}$$

Here, b_i is the true label, $\hat{b}_i^{(q-1)}$ is the prediction at the *(q-1)*th iteration of the q^{th} instance, and $f_q(a_i)$ refers to the q^{th} iteration tree output. [51] Replacing mean square error (MSE) with the loss function, we get:

$$obj^{(q)} = \sum_{i=1}^{n} (b_i - \left(\hat{b}_i^{(q-1)} + f_q(a_i)\right))^2) + \sum_{i=1}^{q} R(f_i)$$

$$= \sum_{i=1}^{n} \left(2 * (b_i - \hat{b}_i^{(q-1)}) f_q(a_i)\right) + f_q(a_i)^2 + \sum_{i=1}^{q} R(f_q) + constant \tag{5}$$

For other losses of interest, like logistic loss, the form of equation might not be sequential as shown. To overcome this situation, second order Taylor expansion of loss function [50] is taken.

$$obj^{(q)} = \sum_{i=1}^{n} L\left((b_i - \hat{b}_i^{(q-1)}) + x_i f_q(a_i) + \frac{1}{2} y_i {f_q}^2(a_i)\right) + \sum_{i=1}^{q} R(f_q) + constant \tag{6}$$

$$\text{Where, } x_i = \partial \hat{b}_i^{(q-1)} L\left(b_i, \hat{b}_i^{(q-1)}\right)$$

$$y_i = \partial^2 \hat{b}_i^{(q-1)} L(b_i, \hat{b}_i^{(q-1)})$$

Here, x_i and y_i refer to the first and second order gradient statistics on the loss function. Equation 7 denotes the specific objective at q^{th} step, all constants are removed, and as a result, we obtain the optimized version of the new tree, where the values of the objective function only rely on the x_i and y_i .

$$obj^{(q)} = \sum_{i=1}^{n}\left(x_i f_q(a_i) + \frac{1}{2} y_i {f_q}^2(a_i)\right) + \sum_{i=1}^{q} R(f_q) \tag{7}$$

γ is the dependent variable of training set and parameters, and the higher the value of it is, the higher regularization it will have. Now, if z denotes the vector scores on the leaves, and N is the number of leaves, then in XGBoost, $R(f_q)$ can be written as:

$$R(f_q) = \gamma N + \frac{1}{2}\lambda \sum_{j=1}^{N} {z_j}^2 \tag{8}$$

From Equation 7,

$$\left.\begin{aligned} obj^{(q)} &= \sum_{i=1}^{n}\left(x_i f_q(a_i) + \frac{1}{2} y_i {f_q}^2(a_i)\right) + \left(\gamma N + \frac{1}{2}\lambda \sum_{m=1}^{N} {z_m}^2\right) \\ &= \sum_{m=1}^{N}\left[\left(\sum_{i \epsilon I_m} x_i\right) z_m + \frac{1}{2}\left(\sum_{i \epsilon I_m} y_i + \lambda\right) {z_m}^2\right] + \gamma N \\ &When,\ X_m = \sum_{i \epsilon I_m} x_i, \\ &\qquad Y_m = \sum_{i \epsilon I_m} y_i \\ &= \sum_{m=1}^{N}\left[X_m z_m + \frac{1}{2} Y_m {z_m}^2\right] + \gamma N \end{aligned}\right\} \tag{9}$$

Here, $X_m z_m + \frac{1}{2} Y_m {z_m}^2$ is the quadratic and z_m are quite independent of everyone. The best z_m and object reduction equations for any given structure can be defined as:

$$\left.\begin{aligned} z_m &= -\frac{X_m}{Y_m + \lambda} \\ obj^{(q)} &= -\frac{1}{2}\sum_{m=1}^{N} \frac{{X_m}^2}{Y_m + \lambda} \end{aligned}\right\} \tag{10}$$

For any tree structure, summing up the statics of x_i and y_i on their belonging leaves, and using Equation 10, the score can be obtained to determine how good the structure is where smaller scores are counted as the better structure. To measure how good the tree is, we calculate *Gain* [52] implementing Equation 11 dividing one leaf into two leaves where the main goal is to optimize one level of a tree at a time. If the output of *Gain* is lower than γ, then no branch will be added.

$$Gain = \frac{1}{2}\left(\frac{X_L}{Y_L + \lambda} + \frac{{X_R}^2}{Y_R + \lambda} + \frac{(X_R + X_L)^2}{Y_R + Y_{L+} \lambda}\right) - \gamma \tag{11}$$

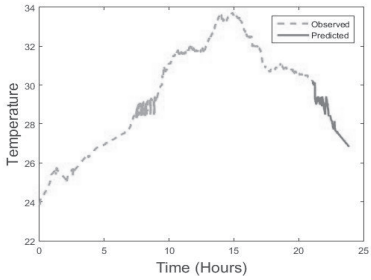
4. Analysis of Processes

The proposed model of blockchain module is applied in six nodes, based on two different private platforms, named Hyperledger Sawtooth and Ethereum. Because of the dissimilar level of customization for storing ledgers [1] and delivering complex logics. When Hyper Sawtooth permits a custom transaction structure, Ethereum[53] [54] [55] works with a single transaction structure. Configuring both networks in a default setting, both of these are compiled in the same computer, one-by-one, where the configuration of the computer is - Intel(R) Core (TM) i3-7130U CPUs with 2.70 GHz, 8 GB RAM, 128GB SSD, 1TB GB HDD, with a newly-installed Windows 10 operating system. We deployed and tested more than 200 scenarios, one-by-one in each platform, where we measured latency, which is time consuming, to set the values in blockchain, CPU load by observing the processing power of every node of blockchain, and network usage by monitoring the bytes transmitted and received. Table I shows the comparison result of Hyperledger Sawtooth and Ethereum, based on the three parameters where Hyperledger Sawtooth gives better performances at every stage.

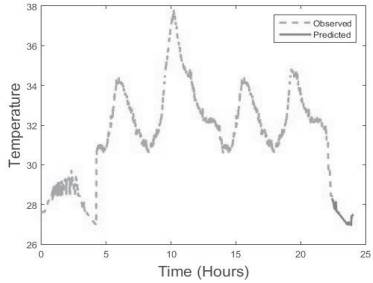
Table I: Performance comparison between Hyperledger Sawtooth and Ethereum

Platform	Memory usages (%)	Latency (second)	Rx (bytes)	Tx (bytes)
Hyperledger Sawtooth	7.08	0.63	32.64	26.33
Ethereum	54.48	22.29	488.95	486.05

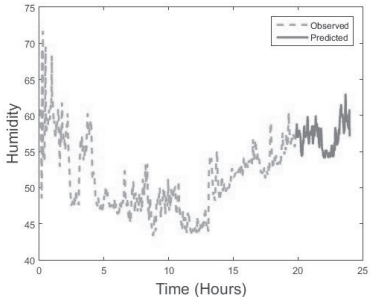
We applied the XGBoost algorithm for predicting future environmental parameters, based on the sensor nodes of two places, and historical data of the urban population, obtained from the World Bank's website, shown in Figure 6. The data, which were acquired during mid-April of 2018, are obtained from two areas named Gazipur and Mohakhali, are predicted for making product distribution decisions where: Figures 6a and 6b are temperature; Figures 6c and 6d are air humidity; Figures 6e and 6f are CO_2; Figures 6g and 6h are O_2; Figures 6i and 6j are soil moisture; and Figure 6k is the statistical visualization of urban population increase in the last 50 years. The graphs are plotted predicting each day's environmental values, where, based on the training dataset and previous data of 18 hours of a day, it predicts the next six hours for demonstration.


Observed
Predicted
Temperature
Time (Hours)

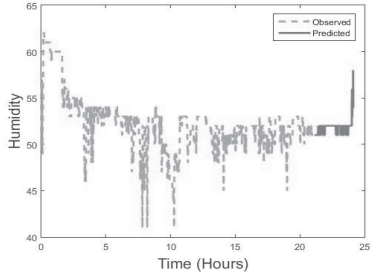
(a)


Observed
Predicted
Temperature
Time (Hours)

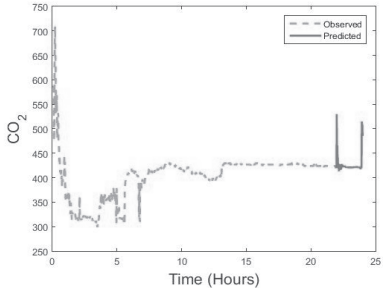
(b)


Observed
Predicted
Humidity
Time (Hours)

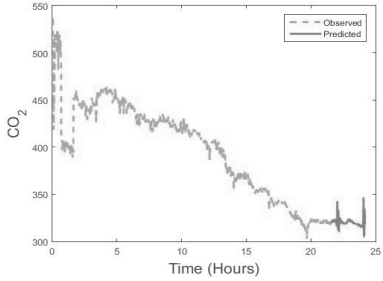
(c)


Observed
Predicted
Humidity
Time (Hours)

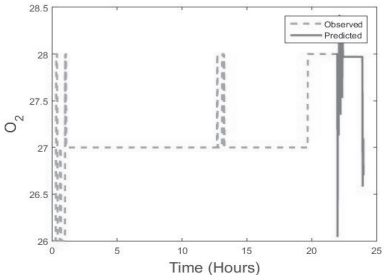
(d)


Observed
Predicted
CO2
Time (Hours)

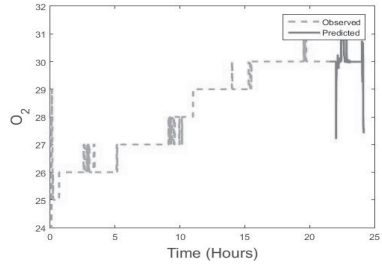
(e)


Observed
Predicted
CO2
Time (Hours)

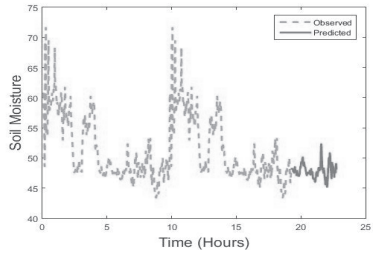
(f)


Observed
Predicted
O2
Time (Hours)

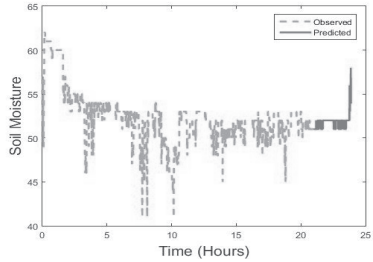
(g)


Observed
Predicted
O2
Time (Hours)

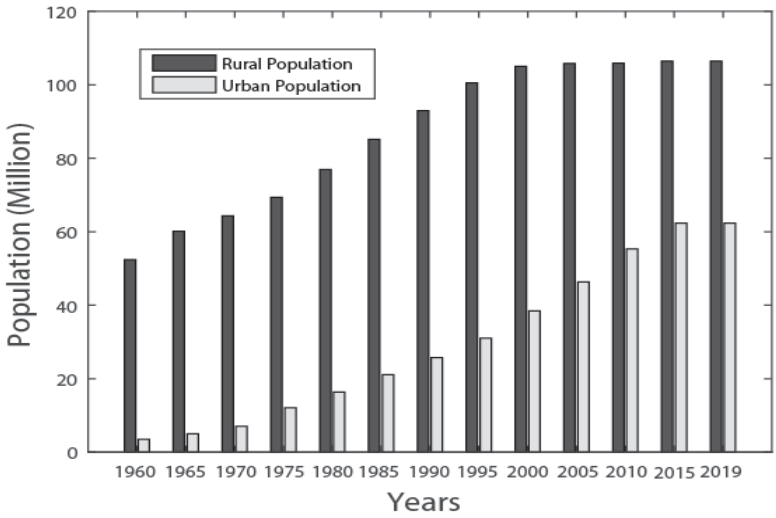
(h)



(i)



(j)



(k)

Figure 6. Predicted temperature of: (a) Gazipur; (b) Mohakhali; predicted air humidity of: (c) Gazipur; (d) Mohakhali; predicted CO_2 of: (e) Gazipur; (f) Mohakhali; predicted O_2 of: (g) Gazipur; (h) Mohakhali; predicted soil moisture of: (i) Gazipur; (j) Mohakhali; and (k) visualization of population in urban area.

Based on the real-time monitored predicted values, early decisions can be made, as changes in environmental parameters affect harvesting. Moreover, from the pH sensor observation, the average pH value of area 1's soil is 5.48, and area 2's soil is 4.97. If the pH value is less than 3.5 or more than 8, it defines a root damage warning, if the pH is between 4 to 4.5 or 7.5 to 8 this denotes poor nutrients of plants, pH between 6 and 7 is an acceptable value, and between 5 and 5.8 is good pH for plants.[56]

Based on that, it can be said that the observed pH value of area 1 and 2 is at the 'almost good' and 'balanced' level, which is efficient for good harvesting.

The performance of the prediction system implementing XGBoost algorithm is analyzed using MSE (mean absolute error) by calculating the error in the prediction values obtained by the trained dataset, compared with the test dataset.

Table II: Average accuracy comparison

Algorithm	Accuracy (%)
XGBoost*	98.78
Linear Regression	94.18
Logistic Regression	92.72
Naïve Bayes	93.09
Neural Networks	97.5

Table II shows the average accuracy of XGBoost compared to other regression algorithms, based on our dataset where all algorithms show good accuracy, but XGBoost obtains the highest average accuracy (98.78%) to predict all parameters.

5. Conclusion and Future Works

The blockchain-based agro supply chain model has the potential and ability to be widely accepted, and to replace the conventional supply chain model, due to its user-friendliness and transparency. In this paper, we propose a comprehensive framework of a smart agricultural supply chain model based on blockchain and the IoT. Moreover, to ensure security and prevent illegal interference, the private database-based blockchain platforms work by limiting user access, with a view to disclosing the huge amounts of data which are needed for AI-based prediction systems for most accurate analytics and suggestion making. The model is capable of providing accountability and transparency, and minimizing the fraudulent activity of middlemen in the food chain network. We tested our system on two platforms for performance comparison. Based on the numerical results, it is shown that XGBoost achieves 98.78% accuracy, which is the highest among other algorithms. The framework is best suited for south and south-east Asian countries, for a transparent system in agriculture, from the field to the hands of customers, as farmers, especially those from

India, Bangladesh and Pakistan, don't get the proper value of their production, but the prices of those products rise many times higher, and thus create economical imbalance. The secure blockchain model, integrating with artificial intelligence and the internet of things, can be a worthwhile model for price equilibrium, practicing a balancing farming culture, and ensuring the best quality of mass-produced products.

For further improvement, many efficiencies are planned, and in the development phase, will be proposed and demonstrated. One of the core components is the graphical user interface (GUI) for all characters. The GUI will be developed in both android application and web versions, for different purposes, with decentralized database. As the farmers or village brokers of the south Asian region may not be used to these applications, a 'tap to listen and write' version of the android application will be presented, so that they can easily understand real-time weather updates and the predicted value of parameters suggested from the proposed artificial intelligence suggester, and trace the supplements. To improve the performance of blockchain in large fields of application, there are platforms like Algorand, with powerful server side processing. Additionally, the development of the IoT section is designed along with fog computing, for faster secure data exchanging. Furthermore, we will extend our study to industry-based supply chain models, and explore enterprise-based smart chain models for agriculture, industry, automation, etc.

References

[1] M. P. Caro, M. S. Ali, M. Vecchio and R. Giaffreda, "Blockchain-based traceability in agri-food supply chain management: a practical implementation," IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany), Tuscany, pp. 1-4, 2018

[2] A. McLean, "IoT security spending to reach $348m in 2016: Gartner," ZDNet, 26-Apr-2016. [Online]. Available:

[3] https://www.zdnet.com/article/iot-security-spending-to-reach-348m-in-2016-gartner/. [Accessed: 25-Nov-2018].

[4] D. Galvin, "IBM and Walmart: Blockchain for Food Safety", [Online]. Available: https://www01.ibm.com/events/wwe/grp/grp308.nsf/vLookupPDFs/6%20Using%20Blockchain%20for%20Food%20Safe%202/$file/6%20Using%20Blockchain%20for%20Food%20Safe%202.pdf [Accessed: 17-Nov-2018].

[5] N. M. Kumar and P. K. Mallick, “Blockchain technology for security issues and challenges in IoT,” Procedia Computer Science, vol. 132, pp. 1815–1823, 2018.
[6] Feng Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & internet of things," International Conference on Service Systems and Service Management, Dalian, pp. 1-6, 2017.
[7] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi and J. Wang, "Untangling blockchain: a data processing view of blockchain systems," IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, pp. 1366-1385, 2018.
[8] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras and H. Janicke, "Blockchain technologies for the internet of things: research issues and challenges," IEEE Internet of Things Journal, 1-1, 2018.
[9] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang, and X. Cheng, “NormaChain: a blockchain-based normalized autonomous transaction settlement system for IoT-based e-commerce,” IEEE Internet of Things Journal, 2018.
[10] K. Leng, Y. Bi, L. Jing, H.-C. Fu, and I. V. Nieuwenhuyse, “Research on agricultural supply chain system with double chain architecture based on blockchain technology,” Future Generation Computer Systems, vol. 86, pp. 641–649, 2018.
[11] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, “Blockchain and IoT integration: a systematic survey,” Sensors, vol. 18, no. 8, p. 2575, 2018.
[12] S. Wang, S. Zhu, and Y. Zhang, “Blockchain-based Mutual Authentication Security Protocol for Distributed RFID Systems,” 2018 IEEE Symposium on Computers and Communications (ISCC), 2018.
[13] 10. “Top five blockchain benefits transforming your industry,” Blockchain Pulse: IBM Blockchain Blog, 03-Dec-2018. [Online]. Available: https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/. [Accessed: 03-Jul-2018].
[14] A. R. Biswas and R. Giaffreda, "IoT and cloud convergence: opportunities and challenges," IEEE World Forum on Internet of Things (WF-IoT), pp. 375-376, 2014.
[15] J. Mesquita, D. Guimaraes, C. Pereira, F. Santos, and L. Almeida, “Assessing the esp8266 wifi module for the internet of things,” IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 784-791, 2018.

[16] "NodeMCU ESP8266 Lua WiFi Internet Development Board". [Online]. Available: https://dealbest.net/transmitters-receivers-module/nodemcu-esp8266-lua-wifi-internet-development-board.html. [Accessed: 17-Aug-2018].
[17] A. Disale, "Eco - A Smart Garbage Container," Hackster.io, 05-Jun-2018. [Online]. Available: https://www.hackster.io/alpha007/eco-a-smart-garbage-container-70094e. [Accessed: 23-Sep-2018].
[18] S. M. Kamruzzaman, M. I. Pavel, M. A. Hoque, and S. R. Sabuj, "Promoting greenness with IoT-based plant growth system," Computational Intelligence and Sustainable Systems EAI/Springer Innovations in Communication and Computing, pp. 235–253, 2018.
[19] "DHT22 Temperature-Humidity Sensor," Techshopbd. [Online]. Available: https://www.techshopbd.com/product-categories/temperature/2806/dht22-temperature-humidity-sensor-techshop-bangladesh. [Accessed: 17-Mar-2018].
[20] "Gas Sensor Module (MQ-135)," Techshopbd. [Online]. Available: https://www.techshopbd.com/product-categories/gas/1624/gas-sensor-module-mq-135-techshop-bangladesh. [Accessed: 23-Mar-2018].
[21] Grove O_2 gas sensor, [online] Available at: https://www.robotshop.com/en/grove-o-gas-sensor.html [Accessed: 17-Mar-2018].
[22] "PH Sensor with Module," Techshopbd. [Online]. Available: https://www.techshopbd.com/product-categories/meters/2576/ph-sensor-with-module-techshop-bangladesh. [Accessed: 17-Mar-2018].
[23] "RFID Starter Kit," Techshopbd. [Online]. Available: https://www.techshopbd.com/product-categories/starter-kits/1299/rfid-starter-kit-techshop-bangladesh. [Accessed: 01-Aug-2018].
[24] "SparkFun Load Cell Amplifier - HX711," Techshopbd. [Online]. Available: https://www.techshopbd.com/product-categories/breakout-boards/2517/sparkfun-load-cell-amplifier-hx711-techshop-bangladesh. [Accessed: 01-Aug-2018].
[25] R. Vrijhoef, "Co-makership in construction: Towards construction supply chain management‖", Thesis of Graduate Studies, Delft Univ. ofTechnology and Technical Research Centre of Finland, Espoo, Finland, 1998.
[26] A. Meola, "How IoT logistics will revolutionize supply chain management," Business Insider, 21-Dec-2016. [Online]. Available: https://www.businessinsider.com/internet-of-things-logistics-supply-chain-management-2016-10. [Accessed: 12-Aug-2018].

[27] M. Abdel-Basset, G. Manogaran, and M. Mohamed, “Internet of Things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems,” Future Generation Computer Systems, vol. 86, pp. 614–628, 2018.
[28] Ucot, “An Introduction to Internet of Things (IoT) in the Supply Chain,” Medium, 13-Nov-2018. [Online]. Available: https://medium.com/ucot/an-introduction-to-internet-of-things-iot-in-the-supply-chain-f0db2a496689. [Accessed: 29-Nov-2018].
[29] V. Dhillon, D. Metcalf, M. Hoope, "The hyperledger project," Blockchain Enabled Applications, pp. 139-149. Apress, Berkeley, CA, 2017.
[30] T. McConaghy, R. Marques, A. Müller, D. D. Jonghe, G. McMullen, R. Henderson, S. Bellemare, and A. Granzotto, "BigchainDB: a scalable blockchain database," white paper, BigChainDB, 2016.
[31] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, “Applications of blockchains in the internet of things: a comprehensive survey,” IEEE Communications Surveys & Tutorials, pp. 1–1, 2018.
[32] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng and V. C. M. Leung, "Decentralized applications: the blockchain-empowered software system," IEEE Access, vol. 6, pp. 53019-53033, 2018.
[33] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, “On Security Analysis of Proof-of-Elapsed-Time (PoET),” Lecture Notes in Computer Science Stabilization, Safety, and Security of Distributed Systems, pp. 282–297, 2017.
[34] G. Dhameja, “Bigchaindb integrates with hyperledger fabric,” The bigchainDB Blog, 12 Sep., 2018. [Online]. Available: https://blog.bigchaindb.com/bigchaindb-hyperledger-fabric-integration-4c65e5811671. [Accessed: 14-Nov-2018].
[35] M. E. Peck, “Blockchains: How they work and why theyll change the world,” IEEE Spectrum, vol. 54, no. 10, pp. 26–35, 2017.
[36] T. Aste, P. Tasca, and T. D. Matteo, “Blockchain technologies: the foreseeable impact on society and industry,” IEEE Computer, vol. 50, no. 9, pp. 18–28, 2017.
[37] J. F. Galvez, J. Mejuto, and J. Simal-Gandara, “Future challenges on the use of blockchain for food traceability analysis,” Trends in Analytical Chemistry, vol. 107, pp. 222–232, 2018.
[38] J. Hua, X. Wang, M. Kang, H. Wang and F. Wang, "Blockchain based provenance for agricultural products: a distributed platform with duplicated and shared bookkeeping," 2018 IEEE Intelligent Vehicles Symposium, Changshu, pp. 97-101, 2018.

[39] C. Xie, Y. Sun and H. Luo, "Secured data storage scheme based on blockchain for agricultural products tracking," 3rd International Conference on Big Data Computing and Communications, Chengdu, pp. 45-50, 2017.

[40] A. S. Patil, B. A. Tama, Y. Park, and K.-H. Rhee, "A framework for blockchain based secure smart greenhouse farming," Advances in Computer Science and Ubiquitous Computing Lecture Notes in Electrical Engineering, pp. 1162–1167, 2017.

[41] Y.-P. Lin, J. Petway, J. Anthony, H. Mukhtar, S.-W. Liao, C.-F. Chou, and Y.-F. Ho, "Blockchain: the evolutionary next Step for ICT e-agriculture," Environments, vol. 4, no. 3, pp. 1-13, 2017.

[42] A. S. Patil, B. A. Tama, Y. Park, and K.-H. Rhee, "A Framework for Blockchain Based Secure Smart Green House Farming," Advances in Computer Science and Ubiquitous Computing Lecture Notes in Electrical Engineering, pp. 1162–1167, 2017.

[43] "What Is Hashing? Under The Hood Of Blockchain," Blockgeeks. [Online]. Available: https://blockgeeks.com/guides/what-is-hashing/. [Accessed: 24-Aug-2018].

[44] H. Gilbert and H. Handschuh, "Security Analysis of SHA-256 and Sisters," Selected Areas in Cryptography Lecture Notes in Computer Science, pp. 175–193, 2004.

[45] "Bangladesh," Data. [Online]. Available: https://data.worldbank.org/country/Bangladesh. [Accessed: 25-Oct-2018].

[46] T. Chen and C. Guestrin, "XGBoost," Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 785-794, 2016.

[47] X. Gao et al., "An improved XGBoost based on weighted column subsampling for object classification," 4th International Conference on Systems and Informatics (ICSAI), Hangzhou, pp. 1557-1562, 2017.

[48] J. Guo, L. Yang, R. Bie, J. Yu, Y. Gao, Y. Shen, and A. Kos, "An XGBoost-based physical fitness evaluation model using advanced feature selection and Bayesian hyper-parameter optimization for wearable running monitoring," Computer Networks, vol. 151, pp. 166–180, 2019.

[49] X. Shi, Q. Li, Y. Qi, T. Huang and J. Li, "An accident prediction approach based on XGBoost," 12th International Conference on Intelligent Systems and Knowledge Engineering (ISKE), Nanjing, pp. 1-7, 2017.

[50] "Introduction to Boosted Trees, [Online]. Available:

https://xgboost.readthedocs.io/en/latest/tutorials/model.html. [Accessed: 21 Aug., 2018].
[51] X. Gao et al., "An improved XGBoost based on weighted column subsampling for object classification,"4th International Conference on Systems and Informatics, Hangzhou, pp. 1557-1562, 2017.
[52] T. Moller, R. Machiraju, K. Mueller and R. Yagel, "Evaluation and design of filters using a taylor series expansion," IEEE Transactions on Visualization and Computer Graphics, vol. 3, no. 2, pp. 184-199, 1997.
[53] "Boosting algorithm: XGBoost," Towards Data Science, 14-May-2017. [Online]. Available: https://towardsdatascience.com/boosting-algorithm-xgboost-4d9ec0207d. [Accessed: 22-Jul-2018].
[54] E. F. Kfoury and D. J. Khoury, "Secure end-to-end volte based on ethereum blockchain," 41st International Conference on Telecommunications and Signal Processing, Athens, pp. 1-5, 2018.
[55] D. Vujičić, D. Jagodić and S. Ranđić, "Blockchain technology, bitcoin, and ethereum: a brief overview," 17th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, 2018, pp. 1-6.
[56] V. Buterin, "Etherium white paper," [Online] Avaiable: github.com/ehthereum/wiki/white paper [Accessed: 29 Aug., 2018].
[57] M. I. Pavel, S. M. Kamruzzaman, S. S. Hasan, S. R. Sabuj, "An IoT based plant health monitoring system implementing image processing" IEEE 4th International Conference on Computer and Communication Systems, Singapore. (In press)

Authors Biography

Md Monwar Jahan Chowdhury was born in a beautiful city named Chittagong, Bangladesh. He completed his B.Sc degree in Electronics & Communication Engineering from BRAC University, Bangladesh. His area of interest and research includes wireless sensor networks, Internet of things, wireless communication, cognitive radio network, block chain etc. He has presented his paper in conferences and journals both home and abroad. He is currently serving in a telecommunication firm under the RF measurement and EMF testing division. His current research work includes investing the bidirectional communication in cognitive radio network.

Monirul Islam Pavel passed SSC and HSC from CUET School and College under Chittagong education board. He has completed Bachelor of Science in Computer Science and Engineering from BRAC University in December, 2018. He is the former director of Robotics Club of BRAC University (ROBU) and lead person of image processing in Computer Vision and Intelligent System (CVIS) research lab. He attended many national and international competition and conferences. Mr. Pavel is current working in Signal Stream Inc as an embedded Software Engineer. His research fields are computer vision, machine learning, deep learning, IoT, robotics, embedded system.

Saifur Rahman Sabuj was born in Manikganj and he passed his S.S.C and H.S.C from Dhaka Residential Model College and completed his B.Sc degree from the Military Institute of Science and Technology, Dhaka University. He completed his M.Sc. degree from Bangladesh University of Engineering and Technology and completed his PhD degree from Kochi University of Technology, Japan. From 2008 to 2013, he was a faculty member of Green University of Bangladesh, Metropolitan University, Sylhet and Bangladesh University. Currently he is working as an assistant professor at department of Electrical and Electronic Engineering, BRAC University. His research interests include MIMO-OFDM, Cooperative Communication, Cognitive Radio and Internet of things for wireless communications.

CHAPTER NINE

EXPLORING E-COMMERCE IN CYBER SECURITY CONTEXT THROUGH BLOCKCHAIN TECHNOLOGY

MD HASAN FURHAD[1], SHAHRIN SADIK[2], MOHIUDDIN AHMED[3] AND ABU S.S.M. BARKAT ULLAH[1]

[1]Centre for Cyber Security and Games, Canberra Institute of Technology, Australia
[2]Department of Computer Engineering, International Islamic University Chittagong, Bangladesh
[3]Academic Centre of Cyber Security Excellence, School of Science, Edith Cowan University, Australia

Abstract

E-commerce is the electronic trade of products over the internet. With the increase in demand for e-commerce in the current world, it is becoming more and more significant to keep the data secured from all malicious attacks. Since the e-commerce business fully depends on reliability and trust, this system needs a highly secure, technical way to sort out all the unsecured issues involved with trade over the internet. To maintain the privacy of the data, it is necessary to keep hold of the capacity of data storage by providing a system which will not only secure the involved data, but will also enable any unauthorised access to intrude into the system and tamper with the data. Blockchain has been the emerging technology which can now be used as an alternative for cyber security. The need for cyber security in e-commerce is very much required, and blockchain is the technology which can contribute in boosting the cyber security for the purpose. These vital features, decentralisation and immutability, are the main aspects of this nascent technology which are

being utilised to make every transaction in the chain clean, easy, and transparent. Despite having the IoT and cloud computing as alternatives for the same purpose, that of providing cyber security in the context of e-commerce, blockchain will prove to be the best choice of all. Every technology has both its good and bad impacts, and so have the other two security versions used in e-commerce: IoT and cloud computing, but blockchain, because of its nature and the encryption technology, is providing a step further than what is expected. The encryption technique used in blockchain makes online trade in e-commerce easier and more confidential, as it provides the opportunity for both the store owner and the customer to keep their agreement or chats private, unless anyone needs to declare them publicly. Exploring e-commerce in the cyber security context through blockchain technology can be very beneficial for the e-commerce society, as it promises to provide all the necessary safety precautions before a trade is made, and even after the trade has been done. This will elevate the experience of the e-commerce platform for both end users and business owners, and make significant advances in this vital field in the current technological world.

Keywords: Blockchain, e-commerce, e-commerce challenges, cyber security, disrupting technology, IoT, cloud computing, security measures, mitigating threats, web security.

1. Introduction

Over the years, leveraging the advantages of the internet has seen a significant increase in different online activities, such as e-commerce. People from all over the world can perform their daily activities, e.g., checking bank transactions, online shopping, and increasing their e-commerce business. In today's society, these activities involve more interconnected, pervasive, and compassionate bonding between the individuals around the globe. [1-2] However, these increasing activities lead to the threat of cyber-crime and various security incidents, and one of the biggest challenges is to develop a secure and privacy-aware environment which can provide high quality e-commerce service.

In recent years, a wide range of concepts has emerged, such as cloud computing, edge computing, the internet of things (IoT), blockchain, etc. to deal with cyber-security-related issues. Among these disruptive technologies, blockchain is gaining more attention and being studied in different fields. Blockchain is a decentralized distributed database

technology which updates the database continuously. [3] It has been observed that addressing the cyber security challenge for e-commerce by exploiting blockchain technology has not been thoroughly studied. Yet blockchain, in its recent developing stage, promises to bring revolutionary change in the field of e-commerce. It is expected to make trade easier for every buyer and seller involved. This chapter will bridge this gap in the literature, and contribute to tackling e-commerce security issues by studying blockchain technology.

2. E-Commerce Background and Operation

According to the definition of the tech target network, [4] 'e-commerce' (EC), an abbreviation for electronic commerce, is the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet. E-commerce is managing and maintaining all the business transactions via telecommunication media. It allows direct connection between buyers and sellers, allowing global connectivity. It aids in supporting customer behaviour by providing interactivity and adapting customer needs. E-commerce enables suppliers to get the best products from the global network without creating any barriers between their requirements and their location. [5-6] E-commerce comprises three basic components: a front web server; a database system; and a dispatch system which links the production house and keeps track of all the goods involved goods, and each and every buyer and seller. There are four types of e-commerce; [7] business-to-business (B2B), business-to-consumer (B2C), business-to-employee (B2E), and customer-to-customer (C2C). B2B is the greatest model of e-commerce which defines two different entities, such as buyer and seller. B2C is basically the selling of products to customers online. B2E is the form which deals with the business of rendering products or services to employees. Finally, C2C motivates person-to-person transactions on a daily basis.

The internet of things (IoT) is the infrastructure which merges hardware, software, and the network to render a clean service to the world, by holding all data in the cloud and allowing regular connectivity and adaptability of data. This creates scope for a customer-centric business approach. Nowadays, online business is in a flourishing state, infusing the IoT in every field, and keeping constant records of trade in the cloud. [8-10] With the help of the IoT, it is becoming easier to handle all the relevant jobs, such as optimising business processes, automating services,

and simplifying buying procedures and decision-making. The IoT can help e-commerce in the following ways:

- For small start-up businesses, products might be fewer in number, but with increasing demand, the need to re-stock increases. Thus, the maintenance of the production equipment and machinery rapidly increases. Here, the IoT contributes to the business by alerting the business to necessary maintenance issues, and allowing sensors, fixed in the machines, to send automated information on any repair or renewal needed. This elevates the simple business idea to an interactive business where there is a complete interaction between the demand, and the need to fulfil the requirements of both retailers and customers.

- The IoT allows the automated purchasing of products for customers, in case they are out of stock of their daily essentials.

- The IoT in e-commerce helps with critical decision-making, depending on the criteria of the business and the protocols needed for every transaction involved. [10] For example, in the case of a natural disaster or calamity, there might be delays in shipping products or delivering them. In this case, the IoT serves to notify customers and retailers about the delay, and the whereabouts of the products, thus boosting an interactive business relationship between them.

There has already been a proposed architecture [11] in the previous work of combined blockchain and IoT, which uses a communication model comprising of peer-to-peer messaging, distributed data sharing and autonomous coordination of devices. This blockchain network involves the implementation of mining, ledger, and encryption, etc.

3. Flaws of E-commerce

E-commerce has made world trade more globally connected, and facilitated every individual to get any required service at home. This, in comparison to regular shopping tendencies, lowers the cost of the products, and even provides 24/7 active service to customers. There is a wider choice of products for customers than in any other marketplaces. However, with every advantage comes a disadvantage, and it is so with the e-commerce platform. With all the flourishing opportunities in this sector,

there are some drawbacks, [12-14] such as the fact that it does not allow the customers to examine the product before purchase. There is a high risk of data security breach, as customers and retailers provide important card details which may play a major role in the data being misused. Most importantly, a regular internet connection is needed to avail the customer of the opportunity of getting into e-commerce, and at times, this is not possible for new internet users. Thus, in a nutshell, e-commerce is a platform which needs major changes in facilitating safe transactions, and more advanced ways to hold the constant attention of customers, to enhance online business. In this perspective, disruptive blockchain technology will definitely play a vital role in changing the e-commerce platform, making it more secure to deal with every transaction, and keep a hold on every customer wisely. This fusion of e-commerce with blockchain will efficiently improve online business, making every buyer and seller trustworthy and reliable, due to the decentralised and immutable nature of blockchain.

3.1 The Importance of E-Commerce Security

Cyber security is the key feature of e-commerce. Without making and implementing proper plans for the security of the online business, the seller gradually puts both himself/herself and the customers at huge risk of fraud. It is important to secure the website for the proper growth of online businesses, due to the high risk of data breaches and tampering with the privacy of the customers. [15] A minimal gap in security may result in huge loss of business, and eventually may even shut down the online store. Online businesses rely absolutely on trust as they deal with payment or financial issues. Thus, any sort of financial mismanagement may create worse situations for both the customer and the online store owner.

4. Blockchain and E-Commerce

Since the invention of blockchain technology, technically literate society has been trying to incorporate it with e-commerce, by means of crypto-currency, and by creating decentralised marketplaces for online businesses.

The following describes the advantages of merging blockchain with e-commerce [16-17] in the online business sector, accelerating the security, needs, and economy, of retailers and customers:

- Amalgamation of blockchain and e-commerce is expected to result initially in decreasing the processing fees of all online transactions. The security standards needed for this will also be elevated, so as to allow the traders to gain the best outcome from frequent use.

- Keeping track of the supply chain of traded products is very important, as the path from retailer to customer includes several hurdles to be overcome. But by involving blockchain in this regard, it will become easier for each of them to keep a track of products, from being produced until they are delivered to the customers.

- Blockchain, with the help of its unique feature, smart contract, will allow control of stock, and will easily notify retailers that pre-defined limits have been reached. This involves helping the retailers to manage the inventory. E-commerce and blockchain together will help businesses to expand, and allow the controlling of the stock by regularly notifying whether products are available or out of stock.

- Due to the immutable property of blockchain, the e-commerce platform in the future will have no security risks concerned with the private details of customers or retailers, as customers need to provide their credit card numbers and personal information for any online transaction and retailers also have their own necessary stock data stored in the database. Compared to the decentralised database, the traditional database has more security risks, and has major possibilities for encountering situations of data loss. This is where blockchain in e-commerce will contribute, by securing the data tightly, making it impossible for any intruder to tamper with it.

- Buying products brings the headache of storing warranty and guarantee cards for customers. At times it may be impossible for the customers to keep them safely. Blockchain will allow the customers to securely store these cards after the products have been purchased. It will then allow them to keep a track of the proof of ownership of the products, or services rendered, in the e-commerce platform.

- Reviews are a most important part of the e-commerce platform, as the positive reviews of former customers motivate new customers to purchase products. However, the possibility of the genuineness

of these reviews is at stake, because there is no proper guarantee of anonymity. In this case, blockchain will also allow a watch to be kept on the genuineness of the reviews given by the customers, right after purchasing any product. It will also add incentives, as rewards for any reviews they give.

- Crypto-currency methods can be used as an alternative method of payment in the e-commerce platform, as this way is faster and easier than any other payment methods. This also boosts the decrease in processing fees. There is no risk associated with alteration and misuse, as with any alternative payment methods, such as paying with cards.

4.1 How blockchain elevates the concept of e-commerce

As we have already discussed the advantages of combining blockchain and e-commerce in the above section, there are still the aforementioned possible use cases to be discussed more elaborately. The cutting out of the middleman, or third-party, in any transaction in the blockchain will play a major role in the e-commerce platform. It will lessen the extra cost of him/her, and reduce the financial burden in comparison to earlier interventions. Moreover, nowadays, everyone prefers self-service, and wants less intervention from the company's representatives to ease any transaction. The decentralisation feature of blockchain will allow and alleviate cross-border trade. It will eventually lower the cost for consumers and retailers. It will also encourage block-to-block transactions, and will create a vital ecosystem for the same. The ownership of the marketing data will be restored and confirmed. The blockchain ensures the privacy of data, and all other technical private information concerned with the relevant e-commerce platform. There remains no central authority to indulge or observe the data of the company, providing the required consumer protection. The power of controlling data is absolutely at the users' disposal, they are free to manipulate their data, as and when required. It will, in the long run, then accelerate to an extent which will eventually allow simplified card payments on the network. The payment methods will have no specific boundaries, and this will also allow borderless transactions, providing better payment gateways for all. Furthermore, crypto-payments will be one of the easiest and fastest ways for any transaction involved in business. This will elevate the opportunities of blockchain and crypto-linked social payments. As we know, credit cards are one of the easiest ways to make the user prone to

fraud. Chargebacks occur when a bank forcefully reverses the transactions done by a credit card. This is the prime opportunity for fraudsters to use this chargeback, even after products have been delivered and received. The use of crypto currencies makes sure that there is no reversal of payment, and makes the transaction safe and sound, in comparison to the chargeback policy. This combination will protect the business from chargeback fraud in e-commerce platforms. The security of data, overall cost reduction, and final integration with business processes, provided by blockchain, will definitely accelerate its wide opportunities in the field of e-commerce. It will, in the long run, protect the social norms and customs of business involving all customers and companies in this regard, for a safer transaction between them. Blockchain removes all possibilities of human error, which is the initial cause of data breaching, in data storage. This technology is also supposed to provide protected edge computing with authentication, by securing the infrastructure of simple and industrial IoT. It will help to upgrade record management. Several companies are currently looking for a technology which can privately secure the message, or information, exchanged over the internet.

4.2 Applications of Blockchain in E-commerce

Smart contracts, inventory control, supply chain tracking, product description database, and loyalty rewards software, are considered to be the main applications of blockchain in e-commerce. [18] A smart contract allows work to be done depending on pre-defined criteria, removes the need for extra staff, and lessens staff workload. This free time helps the staff to concentrate on the market and growing the business. Inventory control is done with the help of smart contracts. This will make it possible to keep track of products, and replacements can automatically be made when necessary thresholds are reached. It ensures that the online store is never out of stock. Loyalty rewards can also be automated because of smart contracts. These rewards will be given when customers reach certain thresholds of shopping from the online store. This will encourage them to visit the online store again, for happy and satisfactory shopping. Supply chain fraud is also a major concern for companies, but, with the help of blockchain, it is now easier to keep a track of all the traded products. This ensures the transparency of the whole supply chain procedure, keeping a vigilant eye on the vendor and his/her related activities.

In a nutshell, blockchain will elevate safe and easy payments in the e-commerce platform, making each transaction way easier, with added

security reducing the additional costs incurred by several other payment methods. Blockchain technology will also provide a visualisation of transparent and clean supply chain management. This will, very soon, allow us to know the whereabouts, and all the details of the products, especially information about authenticity and fairness in the relevant trade. Moreover, the decentralised nature of blockchain will restrict the ability of hackers to hack the system as a whole. Hacking may affect a little information, but mainly, blockchain technology will keep the maximum amount of information secure from the hacker, by not allowing him/her to access the system. This will surely bring rapid change in the world of e-commerce, by providing the desirable above-mentioned facilities, and a technologically approached marketplace.

5. Comparison of Blockchain and Cloud Computing from the Perspective of Security and Privacy

5.1 Blockchain

Blockchain is a system which is referred to as a decentralised and public digital ledger which does not allow any kind of alteration or breach of data for any user. [3] As it is a public ledger, all the users are notified about any alteration made to the data. This makes it quite impossible for a hacker to change any data of a single user. The data in the blocks are protected by the encryption technique. This encryption technique, in general terms, is used to secure the data through the method of encryption and decryption. This technique basically aids by encrypting the data while it is sent by the sender, before it is decrypted by the recipient when needed. This solid mathematical technique, used in the digital ledger, keeps the data in the blocks of blockchain safe, and protects them from any form of alteration which may harm the users of the chain. [19-20]

5.2 Cloud Computing

This refers to the various services rendered over the internet, such as storage, software development platforms, servers, etc. This technology generally relies on sharing computer resources, instead of having personal resources to handle such applications. It provides services over the internet by demanding payment depending on its usage, and delivering whenever anyone needs the service. [21-22]

5.3 Comparison

The cloud allows better productivity and efficiency, as it contributes to reducing the numbers of hardware units used. This, in comparison to the legacy system, provides cost-effectiveness. It lets the worker work remotely during times of personal hardship. There are three main types of cloud computing services: infrastructure as a service (IaaS); software as a service (SaaS); and platform as a service (PaaS). A cloud computing model always requires the involvement of a provider, or any third-party organization, which specifies the selling of infrastructure as a service (IaaS). IaaS is efficient for temporary and easy-going applications. It aids in dealing with the workloads which are probing, and are prone to unexpected changes.

On the other hand, blockchain technology does not require any third-party support, and restricts the intrusion of any external controlling authority. This is done by providing the ability to possess and verify the data held during any transaction, to all the users.

Cloud computing has public, community, and private deployment models, whereas blockchain has permissioned and permission-free deployment model chains. These chains in blockchain are used to meet the security and privacy requirements.

Both cloud computing and blockchain fully encrypt the data stored within them. But a cyber-risk-free zone is created in cloud computing for keeping data under continual surveillance. Zero security network models are being used by many renowned companies in the case of cloud computing, to restrict any outsiders to access the data. Cloud computing verifies the identity of a person trying to use the resources. The blockchain uses a cryptographic hash function, and this uses a public-private key cryptography technique which ensures the data is received by the intended recipient. This allows the data to be free of interruption, and keeps the data tamper-proof. Both cloud computing and blockchain firmly deal with encountering and strengthening cybersecurity by providing several mechanisms to secure the resources.

5.4 What is Cyber Security?

Cyber security is referred to as the ultimate defence or security mechanism for a number of inter-connected systems. In the context of computing, cyber security comprises physical and cyber security. This basically deals

with guarding the system from various cyber-attacks, as well as preventing unauthorised access to any important computerised system. Application security, information security, network security, end user protection, and operational security, are a few of the key elements of cyber security. The evolution of security risks has become the major concern of cyber security. The involvement of cyber security in every important case can aid in encountering, or even preventing, cyber-attacks, identity theft, and breach of data; significantly contributing to the management of any associated risks. [15,23]

6. Security Risks in E-commerce

Every e-commerce dealer must be aware of the following ten security risks: online security, system reliability, privacy issues, customer disputes, credit card fraud, intellectual property, SEO, taxation, return of goods and warranty, and warehouse and logistics. There are many kinds of security threat, a few of them are accidental, a few are done on purpose, and some are caused due to human error. To protect oneself from any online insecurity, it is important to regularly update the operating system, and make use of a very strong security sockets layer (SSL). It will then prevent the system from being open to various security threats, such as phishing attacks, malware, hacking, and so on. System reliability is something which is out of control at times. Despite keeping all the systems updated on a regular basis, it may become hard to maintain the active reliability status, in terms of the system. The ISP server may crash, or the procedure of online payment may slow down, or error bugs in e-commerce may appear, due to the unreliability of the system. In the case of online businesses, it is necessary to hold on to important data by using strong user passwords. This use of firm passwords initially reduces the possibility of data or identities being stolen and misused. Spamming and unsolicited marketing may also become a concern while handling privacy issues. A situation may arise where a customer has input the card twice, or thrice, or maybe more, but hasn't received products in accordance to their need or demand. It is the prime duty of an online seller to keep the customers satisfied. But these troublesome issues may lead to confusion, where disputes with the customer may occur, resulting in the loss of valid and good buyers. It is possible for any hacker or thief to misuse credit cards if they are stolen. This misuse may lead to great loss of customers. This is the main concern of security, as transactions made cannot be overlooked, and this is almost the most prevailing risk in online businesses of all time. Intellectual property comprises of elements such as your own content,

logos, products, etc., which may be easily replicated by any fraudulent seller. The violation of such property may occur in the context of online business. Websites may, at any time, drop down in the web traffic priority listings, which may incur huge loss. It might happen that the shipping amount, or necessary taxes concerning the products, are not considered sufficiently while selling products online. Moreover, the return of products or delay in product delivery, and out-of-stock products may also lead to severe financial losses for the seller. [24-26]

7. Combating Security Threats in E-commerce

Accurate mechanisms and their implementation are required to protect any system from heinous security threats. This implementation will eventually secure, or reduce the possibilities of, the breaching of security. The security risks can be minimized by involving encryption techniques while transferring data by encoding them, allowing or adding digital certificates by a third-party organisation in order to provide authentication to the website, and keeping an audit check as a routine check-up for the security issues concerning the system. This will surely lead in reducing the security threats to a system.

8. Cloud Computing and E-commerce

Cloud computing is being highly favoured for e-commerce nowadays, due to its four excelling features. Scalability, speed, cost reduction, and redundancy, in cloud services are the four key features of cloud computing which are influencing the e-commerce society, which relies on them. Scalability is a big issue with regard to online business. The necessity of high scale increases with the increase in business, and cloud computing enables the increase or decrease of scale, as per the demand or the traffic congestion of the website. Cloud computing provides better speed than any other services for e-commerce. [21-22] this, in return, boosts the business in high spikes. Speed plays a major role in attracting customers to the website, as it is important to be able to be very fast while conducting any sort of transaction. Due to the pay-as-you-go service of cloud computing, it becomes very convenient for users to render any service, as per their requirements. The development and maintenance procedures of the infrastructure of the technology are being cut down, due to the profound utilisation of cloud-computing for e-commerce. Data backup is very significant in the case of any online business. The customers' data is crucial for an online seller, as it enables the business to be free of any

catastrophic disaster. The built-in redundancy features of cloud computing aid the online business owner to keep track of all the data for any emergency need. Cloud computing is a disruptive technology, which, when combined with e-commerce for the purpose of cyber security, plays a significant role in escalating and acquiring the goals to be accomplished by the e-commerce society. This amalgamation of technology is rapidly changing, and will continue to bring indefinite and beneficial changes in the area of e-commerce. [27-28]

8.1 Challenges of Combining E-commerce and Cloud Computing

Despite various favourable conditions for using cloud services for e-commerce, there are **a** number of issues or challenges to be dealt with on account of it. [29-30] the key challenges are as follows:

- **Data storage:** The inability to store business-based data on the cloud services is a matter of concern for most of its users. It is difficult to control the replication, partitioning, and distribution of data in incorporating cloud services for e-commerce. This inability causes users to be cautious about the procedures and policies of using it.

- **Data privacy:** The necessary technological solutions for the privacy of the data are required in cases of cloud-based e-commerce. It is a matter of great concern to protect the information of companies and their clients.

- **Service quality:** Quality of service (QoS) must guarantee the overall performance, availability, security, dependability, and reliability, for all the services rendered between the cloud and the end users. In this case, QoS in the cloud must offer proper services for the overall performance of both virtualisation and monitoring tools. It is now high time to reduce the uncertainties of QoS.

- **Security:** Security is the biggest drawback of cloud service for any e-commerce application. There is a high chance of third-party intrusion between the inter-relation of e-commerce applications and clients. It is especially high risk when data is created and modified in the cloud. This makes it hard to look for efficient solutions which are also economically wise enough to protect the data and

information from various malicious attacks. There is every possibility of alteration of data, or even deletion, while it is being processed or in transit.

- **Trust and reputation:** Trust has been the biggest challenge so far for cloud computing in the platforms of e-commerce. It becomes difficult for customers to differentiate between a good and bad e-commerce website. This then, acts as a barrier for clients and their companies to completely shift to cloud computing for e-commerce applications.

- **Dependence on connectivity:** The internet is required to access the resources needed for utilisation of such e-commerce platforms. It might not be possible for every end user to be regularly active in time of need, and reliable connections may not always be available, thus making it problematic, and even impossible for the end users to be tethered on a network connection.

- **Service standards issues:** The companies are not usually informed about the policies and procedures of the infrastructure and services used in cloud computing. The specific details about the location, structure, technological situations, staff, and the operational modes, are not communicated to the customers. This might become a matter of hesitation for customers in using and trusting the service.

9. How can Blockchain Help E-commerce by Improving Cyber Security?

E-commerce is the backbone of the recent technological globe, and it is important to make it stronger, just to stand still in the competitive and technical world. Blockchain is the solution for this backbone, it holds e-commerce straight, and makes sure it is firm enough to hold all the necessary information involved in the business. Blockchain technology, which involves smart contracts, enables the e-commerce platform to be more secure, and to concentrate more on the business. It is a trustworthy, highly-influenced technology, on which any of the clients or companies may rely. It provides a number of clean services for both customers and the online store owner. By utilising the smart contract of blockchain technology, it will be possible to restrict any unauthorised access to the network, keeping all the data private and confidential. These smart contracts are computer protocols which are important, and which work at

promoting transactions. This provides transparency in the exchange of all sorts of property, money, goods, services, or anything of esteemed value. Blockchain will also aid in preventing distributed denial of service attacks (DDoS) by fully decentralising DNS, the bulk which stores all data. This is done by distributing the necessary and reliable content into all the nodes, which makes it impossible for the hackers to attack.

10. Conclusion

In the near future, blockchain-based e-commerce will expand the areas of interactivity and connectivity, allowing all the retailers and customers to get involved with each other, from the beginning to the end of each transaction. This will allow a reliable business to occur, with zero percent chance of betrayal in the trading procedure. This will also encourage buyers to depend solely on online businesses, without the fear of any security risk. The privacy of details shared by the involved parties will be assured by the blockchain security features, and the chances of data being altered or changed will be reduced, because of the immutability of blockchain technology. This decentralised and distributed ledger will ensure proper online business, by keeping a constant track of the supply chain management, products delivered, and genuine reviews, and notifying about any mishaps which occur during the procedure. This combination of e-commerce and blockchain is expected to bring a drastic change in the nature of online business, by providing and creating a safer and cleaner environment for the dealers.

References

[1] Gregory, G. D., Ngo, L. V., & Karavdic, M. (2017). Developing e-commerce marketing capabilities and efficiencies for enhanced performance in business-to-business export ventures. *Industrial Marketing Management*.

[2] Mazzarol, T. (2015). SMEs engagement with e-commerce, e-business and e-marketing. *Small enterprise research*, *22*(1), 79-90.

[3] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)* (pp. 557-564). IEEE.

[4] Web Link: https://searchcio.techtarget.com/definition/e-commerce

[5] Gupta, A. (2014). E-Commerce: Role of E-Commerce in today's business. *International Journal of Computing and Corporate Research*, *4*(1), 1-8.
[6] Laudon, K. C., & Traver, C. G. (2018). E-commerce 2017.
[7] Web Link: https://www.slideshare.net/munishsingla71/e-commerce-ppt-10713485
[8] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431-440.
[9] Singh, S., & Singh, N. (2015, October). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 1577-1581). IEEE.
[10] Xu, X. (2014). IOT Technology Research in E-commerce. *Information Technology Journal*, *13*(16), 2552-2559.
[11] Singh, M., Singh, A., & Kim, S. (2018, February). Blockchain: A game changer for securing IoT data. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)* (pp. 51-55). IEEE.
[12] Web Link: https://www.explainthatstuff.com/ecommerce.html
[13] Briones, A. G., Chamoso, P., & BARRIUSO, A. (2016). Review of the main security problems with multi-agent systems used in e-commerce applications. *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, *5*(3), 55-61.
[14] Turban, E., King, D., Lee, J. K., Liang, T. P., & Turban, D. C. (2015). E-Commerce Security and Fraud Issues and Protections. In *Electronic Commerce* (pp. 457-518). Springer, Cham.
[15] Trautman, L. J. (2015). E-Commerce, cyber, and electronic payment system risks: lessons from PayPal. *UC Davis Bus. LJ*, *16*, 261.
[16] Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. *Financial Innovation*, *2*(1), 20.
[17] Zheng, Z., Xie, S., Dai, H. N., & Wang, H. (2016). Blockchain challenges and opportunities: A survey. *Work Pap.–2016*.
[18] Lemieux, V. L. (2016). Trusting records: is Blockchain technology the answer?. *Records Management Journal*, *26*(2), 110-139.
[19] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183-187.
[20] Al-Jaberi, M., Mohamed, N., & Al-Jaroodi, J. (2015, March). e-commerce cloud: Opportunities and challenges. In *2015 international*

conference on industrial engineering and operations management (IEOM) (pp. 1-6). IEEE.

[21] Juncai, S., & Shao, Q. (2011). Based on Cloud Computing E-commerce Models and ItsSecurity. *International Journal of e-Education, e-Business, e-Management and e-Learning*, *1*(2), 175.

[22] Ahmad, T. (2019). Technology Convergence and Cybersecurity: A Critical Analysis of Cybercrime Trends in India. *27th Convergence India Pragati Maidan*, 29-31.

[23] Khan, S. W. (2019). Cyber Security Issues and Challenges in E-Commerce. *Available at SSRN 3323741*.

[24] Smith, S. N., Nah, F. F. H., & Cheng, M. X. (2016, July). The impact of security cues on user perceived security in e-commerce. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 164-173). Springer, Cham.

[25] Neama, G., Alaskar, R., & Alkandari, M. (2016, January). Privacy, security, risk, and trust concerns in e-commerce. In *Proceedings of the 17th International Conference on Distributed Computing and Networking* (p. 46). ACM.

[26] Goel, K., & Goel, M. (2016, May). Cloud computing based e-commerce model. In *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)* (pp. 27-30). IEEE.

[27] Talib, A. M., & Alomary, F. O. (2016, March). Cloud computing based E-Commerce as a service model: impacts and recommendations. In *Proceedings of the International Conference on Internet of things and Cloud Computing* (p. 27). ACM.

[28] Baghdadi, Y. (2013). From e-commerce to social commerce: a framework to guide enabling cloud computing. *Journal of theoretical and applied electronic commerce research*, *8*(3), 12-38.

[29] Saleh, A. A. E. (2012). A proposed framework based on cloud computing for enhancing e-commerce applications. *International Journal of Computer Applications*, *59*(5).

Authors Bibliography

Md Hasan Furhad is working as a Lecturer for the Centre for Cyber Security and Games at Canberra Institute of Technology (CIT), REID Canberra. His research interests include, cyber security, blockchain, e-commerce, web security vulnerabilities. Prior joining to CIT, he completed his PhD from University of New South Wales, Australia in the field of Computational Image Processing. Prior to that he has completed Master by

Research from University of Ulsan, South Korea in the field of Embedded Computer Architecture.

Shahrin Sadik is pursuing Masters at International Islamic University of Chittagong (IIUC) in Bangladesh. Her research interests include blockchain, health care and security.

Mohiuddin Ahmed attained his PhD in Computer Science from UNSW Australia. His research expertise encompasses cyber security and machine learning, and covers a wide range of application domains. Mohiuddin holds over five years of data science and cyber security experience. He is currently working as a Lecturer in Computing and Security Sciences in the School of Science at Edith Cowan University. Prior to joining ECU, he served as a Lecturer in the Centre for Cyber Security and Games at Canberra Institute of Technology (CIT) and was also involved with CIT's Data Strategy Working Group.

Abu S.S.M. Barkat Ullah is heading the department of Cyber security and Games at Canberra Institute of Technology (CIT), REID Canberra. He has completed his PhD from University of New South Wales, Australia. His research interest include cyber security, project management, optimization, blockchain etc.

CHAPTER TEN

BLOCKCHAIN IN HEALTHCARE

SHAHRIN SADIK[1], MOHIUDDIN AHMED[2]
AND MD. HASAN FURHAD[3]

[1]Department of Computer Engineering, International Islamic University Chittagong, Bangladesh
[2]Academic Centre for Cyber Security Excellence, School of Science, Edith Cowan University, Australia
[3]Centre for Cyber Security and Games, Canberra Institute of Technology, Australia

Abstract

Blockchain technology has gathered substantial interest in the healthcare ecosystem. It is rapidly growing in the field of computer science, as it can contribute significantly to improving the quality and efficiency of a system by providing the key factors to ensure the integrity and authenticity of data. It is a new technological revolution, based on the fundamental concept of a distributed ledger, which stores data in a chain of blocks, having a decentralized and immutable database, with minimal scope for tampering. Presently, the healthcare ecosystem is inadequate to introduce the facilities of a secured system which is easily operable, transparent and cost-effective. The blockchain approach offers numerous applications in this sector, starting from an improved public health management system which limits medical negligence, to counterfeit drugs involving smart contracts to automatically bring actions, as per the needed criteria. Blockchain, in today's on-demand digital healthcare industry has some limitations and challenges, and if we are able to overcome these limitations and challenges, then we can connect to a new era of healthcare, facilitating a complete patient-centric system. This chapter aims to contribute towards a comprehensive study of a blockchain technology-articulating healthcare ecosystem, which, in the long run, may bestow the

healthcare world with a technology almost similar to 'Dentacoin', which connects the dental industry with several vital features.

Keywords: Blockchain, computational time, chronological, cryptography, decentralization, Dentacoin, electronic health record (EHR), interoperability, smart contracts, tokenization, etc.

1. Introduction

Blockchain is primarily a chain of blocks which stores important data and takes care of the integrity of these data. They are secured, and cannot be modified once they have been stored. A cryptographic technique is used for securing the data so that they cannot be altered or deleted. It is basically a database, or commonly known as a digital distributed ledger, which records and stores several transactional data between various nodes or computers in the form of blocks. [1] These blocks are time-stamped and interconnected. It is one of those nascent technologies which have the potential to bring about revolutionary change in today's digital world. It can provide a safe and secure way of communication amongst the dealing parties, with a reliable agreement ratified between them.

Blockchain technology promises to remove the inefficacies of third-party dealings for more transparency in the consensus protocol. This will eventually allow a clear and trustworthy transaction. The fundamental reason behind blockchain technology being immutable and distributed is to use the consensus mechanism to proper effect. It is needed to ensure that all the nodes share the same information of any transaction held in any of the nodes. It is also required to verify additions or deletions made to any block of data. The audit trait of blockchain technology ensures data integrity. [2] This trait requires a digital fingerprint to approach further with any dealings in the long run between the parties involved.

This chapter aims to summarize the concept of blockchain technology in the field of healthcare. Section 1.1 directs the reader to the detailed part of how blockchain works, and Section 1.2 aids the reader to know about the driving factors of this technology. Section 1.3 and Section 1.4 covers the basic idea behind blockchain technology: cryptographic process and smart contracts. In the later part of this chapter, Section 2 focuses on all the use cases of blockchain technology. Section 2.2 highlights several uses of this technology in the healthcare system. Section 3 of this chapter finally aims to wrap up the challenges and limitations of it, followed by Section 4,

which concludes the chapter "Combining blockchain technology and the healthcare ecosystem."

1.1. How Blockchain Works

Blockchain basically has three parts, which makes it a concrete technology. These are:

a) It holds information about when and how the transaction occurred.
b) It holds information about the dealers of the transaction.
c) It gives each block a unique identity which segregates one block from the other. This identity is given to each block by the help of the 'hash' function.

A block in a blockchain has a size of about 1Mb, which makes it more compatible to store thousands of small transactions. There are certain criteria which should be followed before adding a block to the blockchain. [3] The following are the key features of blockchain technology which allow it to create a string of multiple blocks:

a) There should be a transaction.
b) The transaction should be verified.
c) Once the transaction is verified, the vital information regarding the transaction, including digital signature and its relevant detail, must be stored in the block.
d) The block involved in the transaction is to be given a unique identifier code, known as hash, to be able to recognize the block.
e) Another hash of the latest block added to the blockchain also needs to be added to the former block for proper serialization.

Finally when a block is added to the blockchain, it is then publicly available to everyone sharing it. Due to adding up blocks in a linear and chronological order in the blockchain, it becomes harder for a miner to disrupt any previous block, or tamper with the data instilled in the block. The above mentioned hash is formed by a mathematical function which consists of a series, or a string, of various letters and numbers i.e. the information in the block. It is nearly impossible for an intruder to tamper with the information, as it continuously changes the hash of the block. [4] The computational time for calculating these hash values of every single block in the blockchain will be very difficult for a hacker. The hacker will certainly fail if he/she tries to disrupt the flow of data, or alter any information of the transaction occurred.

Blockchain technology has gained profound attention in recent times, because of its decentralized nature. It does not depend on any central third party, and offers a database which is transparent and secured. The consensus mechanism used in this technology is supposed to guarantee the alteration or modification of any block in the blockchain. It is only possible if the majority of the peers or nodes across the network agree to it by validating the transaction in the ledger. This, in return, ensures that replication takes place in the network, while any changes are made in the list of transactions. It essentially assures that all the nodes in the network share the same data at a time.

There are two types of participants in the blockchain network, one who can only read, i.e. the reader, and the other who can write, i.e. the writer. The reader here, in the general sense, can only see the ledger, but is unable to edit any required detail, whereas the writer has the opportunity to audit the data. The writer can also bring changes in the list of transactions, as and when required. These participants generally play the vital role in different types of blockchain: permissioned blockchain, and permission-free blockchain. [5] The basic difference between these blockchains is that the former allows anyone in the network to be the reader and writer at any point of time. It makes the blockchain almost a publicly-available ledger without any central authority. On the other hand, permissioned blockchain is the one which allows only a limited number of readers and writers; those who are within the range of a private authority. This private authority determines the right of an individual in the network to be a reader or writer.

1.2. Driving Factors of Blockchain Technology

The driving factors which causes blockchain technology to be considered from an innovative perspective are as follows:

a. Speed and cost effectiveness: blockchain speeds up the work between the dealing parties. It reduces the intervention and involvement of any third party. This tendency eventually increases the effectiveness of the work. It also decreases the overall costs associated with intermediary parties.
b. Security and integrity of data: It is nearly impossible for anyone to interrupt the transaction. It is because the cryptography method involved in blockchain technology makes it particularly difficult to disrupt the information secured in the blocks. Furthermore, the sharing feature of blockchain makes it possible for everyone across

the network to see if any changes are made in the blocks accordingly.

c. Origin and traceability: A chronicle report of all the transactions held from the beginning is stored in the digitally-distributed ledger, i.e. blockchain. It can be easily viewed by anyone when required.

1.3. Cryptographic Process

Asymmetric cryptography has been used in the cryptographic procedure in blockchain technology. It is used to ensure that both the parties involved in the transaction get the opportunity to prove their identity, making it more secure and safe. It is also known as public key cryptography, which primarily includes a public key and a private key. The union of these two keys makes the digital signature. [6] The digital signature allows ownership of the information, or the blocks involved in the digital ledger. This cryptographic pair, the public key with the private key, is mainly used for decryption and encryption of the transaction, respectively. These keys are most importantly used for sharing and signing the transactions across the network to assure its authority. The public key is predominantly shared with everyone, while the private key is only allowed to be used privately. This key-pair can chiefly be thought of as a bank account and its pin number, in the case of employing cryptography in the blockchain. This method of asymmetric cryptography is much more efficient than RSA cryptography. The private key is mainly used to derive the public key, mathematically. This makes it difficult for any hacker to crack it using reverse mathematics, i.e. deriving the private key from the public key. This method also adds in few more necessary measures and steps before finally presenting the public key in the certain network.

The digital signing generally works as follows:

i. The first user generates a transactional hash.
ii. He/she then uses the private key to encrypt this hash to sign the agreement or consensus.
iii. The signed transactional hash as well as the public key of the first user is sent to the second user.
iv. The transactional hash received is regenerated by the second user. This is done after all the prior inputs before hashing were taken by him/her to compare after the hashing is done.
v. The second user, with the help of the public key, decrypts the signed hash received from the first user. This technique uses a cryptographic algorithm for the purpose.

vi. Finally, the second user compares the hash value. He/she then validates and verifies that the first user has the sole authority of the inputs sent to him/her.

Thus, it becomes both practically and financially unreal, as well as computationally challenging, for any intruder to compute the mathematics involved behind finding the private key from the available public key. If by any chance, the private key is lost, then all the information is also supposed to be lost. It technically becomes impossible to get hold of any block without the presence of either of the keys from this key-pair. The proof-of-work is the most significant part of the blockchain technology. [7] It is the consensus algorithm that is primarily used to substantiate the transactions and generate new blocks in the chain. Here, cryptography is majorly used to compute the proof of work function before verifying any block. This contributes to preventing the attackers from altering or editing the transaction details that already exist in the blockchain. This eventually ensures the security and integrity of the data sent and received within the transaction phase.

1.4. Smart Contracts

Smart contracts are the agile programs or lines of code, typically written in JavaScript. Smart contracts are hoarded in the blockchain with the motive of automatically enforcing action when all the pre-agreed terms and conditions are met. It improves efficiency of the programmed process. These contracts are considered to be one of the momentous potentials of blockchain, which intend to ease, authenticate, and implement, the settlement, negotiation, or execution of the contract. [21] The vital aspect of smart contracts is that they do not need the intervention of a mediator to execute their performance. This makes the smart contract cost-effective by minimizing the points of failure and eliminating human error. Basically, the smart contract consists of particular logics in detail. It is meant to provide the contractual terms and conditions needed. This is done before the submission and approval of any action taken, to process the claim between the agreeing parties in real-time, with a view to validating the eligibility of the claim. [8] The prime pinning of smart contracts in the subject of blockchain is the automatic execution of the conventional agreement. This enhances the blockchain technologies in every aspect, providing ways to directly control the asset distribution, as per the requirement. It creates a technical and secure infrastructure for the individuals involved.

Before going into more detail on what the use cases of blockchain technology are, let us see an example of a scenario where blockchain is applied. It may look exactly like the following:

i. A doctor puts forward a claim for the facilities provided to a patient in the blockchain of an insurer.
ii. After the claim is uploaded, a smart contract is activated. It is programmed with relevant business protocols that inspects the claim, and eventually fixes the allowance accordingly.
iii. Lastly, after the completion of the inspection, it prompts an event. This event causes the claim to be paid, as per the business rules prescribed in the smart contract, depending on the type of submitted claim.

Seeing the above mentioned scenario, we can easily understand that there is no human intervention or need for any mediator for the processing of any initial claim submitted for either purpose in the blockchain. This makes the transaction more transparent and error-free. It also reduces the cost associated with any third party, and increases the speed of the whole claim procedure.

2. Use Cases of blockchain

Blockchain, this go-to technology, is playing a significant role in disrupting several industries with its effective nature and the features associated with it. This technology is expected to bring revolutionary change in the digital world. It is expected to minimize the need for a trusted mediator, gradually making every user independent of the third parties involved. [21] This makes it easier for everyone to control the privacy of their personal belongings. Essentially, blockchain in recent times, is not only concerned about the financial dealings and transactions, as per the rulings of bitcoin. It is increasingly expanding beyond the bitcoin technology, with a growth of use cases of blockchain in other industrial areas. Blockchain can be applicable in providing services for banking, real-estate, healthcare, travelling, digital insurance, asset tokenization, supply chain management, digital identity, energy market, smart contracts, digital voting, distributed storage, notary, education, prediction markets, the internet of things, law enforcement, governance, and human resource management.

2.1. Recent Significant Implementations

Bitcoin and Ethereum are the two major implementations of blockchain which involve digital currency. There is a minor difference between the implementations. Bitcoin is a digital currency, whereas Ethereum is a platform where anyone in the peer-to-peer network can develop decentralized applications in blockchain regarding any applicable use case. Ethereum has its own digital currency, named Ether. Primarily, Ethereum also deals with the execution of smart contract applications, which is the prime feature of it. It also allows Ether transactions within the network.

2.2. Use Cases in Healthcare

Healthcare organizations have been facing various vital problems for ages. [2] To cope with the current smart technologies, they are initially working on developing and deploying solutions which can eliminate the existing problems in this prominent sector. It is enhancing the digital world of healthcare and making it more compatible for the doctors, patients, and workers involved in the healthcare ecosystem. The rapid growth of blockchain technology has incentivized the healthcare sector, rendering several applications which have taken the sector by storm. The use of this technology in healthcare aims to retain money, and improve and expand the trust-based business practicing environment. [5] It also will authorize data sharing, as well as implementing a patient-centric ecosystem.

Several initiatives have already been taken to ensure cost reduction, intensify cybersecurity, render personalized treatment, allow access to information, and acknowledge patients through empowerment. The healthcare industry has also a growing demand for asset tracking, as for example, tracking drugs for the assurance of authentication, i.e., auditing supply chain management. It is important to note the main sources of excessive cost in healthcare systems. It essentially covers expensive tests, inadequate treatment, improper medication, fraudulent healthcare, and missing prevention for chronic diseases. As we already know, blockchain is a technology with decentralized, trustless, distributed, and immutable features. Thus, it is appropriately applicable to recover the prevailing situation in the wider healthcare industry through providing ample opportunities to counter the aforementioned concerns. The present field of vision in an inevitable patient-centric healthcare scenario, is that all the participating members will have transparent and seamless involvement. It will be aware of regular health records. This will predominantly serve the

purpose of expanding the anticipation of faithful care coordination in the digital world of healthcare.

The main regions where blockchain is supposed to have considerable possibilities in the developing healthcare industry are as follows:

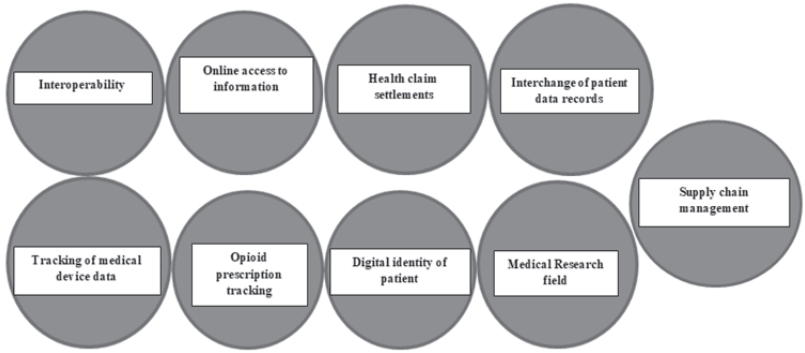


Figure 1 Use Cases of Blockchain in Health Care Ecosystem

i. **Interoperability –** The concept of blockchain interoperability is all about easy communication between the peers involved across the network. According to the definition of interoperability given by the Healthcare Information and Management Systems Society (HIMSS), "Interoperability is the ability of health information systems to work together within and across organizational boundaries in order to advance the effective delivery of healthcare for individuals and communities." With interoperability, blockchain systems adapt the ability to share information within them safely, even if a user from a different blockchain network sends something to a user of another blockchain network. It will then be very easy for the receiver to use and edit the information received. Basically, interoperability in healthcare via blockchain technology can bring in the potential beauty of an ideal healthcare system.[26] It will assure its contribution towards a patient-centric healthcare environment, allowing the patient to access his/her information at any point of service, without the intervention of any mediator. The reason why today's healthcare system is not up to the mark in the arena of interoperability is that the existing healthcare system lacks speed, security, and complete context. Despite knowing the significance of data sharing, the current healthcare system is unable to play a vital role in this case. It is a

coordinator-based system, which is deprived of providing proper facilities needed to enhance a system as per a patient's requirement. It does not allow the patient to have control of his/her own data. It is extremely slow in service, and there is a huge risk of corruption or theft of the patients' data. It does provide fragmented patients' history, which makes it difficult for care providers outside a certain health area to look for, and provide, proper treatment to the patient on an emergency basis.

ii. **Online access to information –** In the present world, it is very important to have substantial access to one's personal health information. But the prevailing healthcare system does not allow the patient to have firm access to it. It has become a global necessity to realign the technical solutions in this regard. Blockchain technology in healthcare is about to provide this opportunity, through its cryptographic method, and via its distributed nature. Here, the patient can access his/her information at any point, and can also allow the care provider of any healthcare organization to get access to the information via the public key of the patient's blockchain system. Let us assume an emergency scenario, supposing that a patient is in dire need to have all his health records, in an emergency situation. [10] As his health deteriorates unexpectedly, and he is unable to reach the hard copies of his health documents, the available doctor has to go through all the test reports. Since not all the documents are on hand, the patient has to go through all the medical tests once again, which ultimately delays the treatment, putting the patient at risk. Whereas, if the available doctor, or the care provider, was able to have access to all his health information on an urgent basis, i.e., when needed, then it would be way easier for the doctor to provide the right treatment, at the right time, to the patient. Subsequently, this is how a blockchain-based healthcare system can aid today's healthcare world, by offering valuable access to the network, securing the integrity of patients' information, and creating an opportunity for patients to carry their medical records when travelling.

iii. **Supply chain management (tracking counterfeit drugs) –** Blockchain in the supply chain management of the healthcare industry will play a transformative role, by keeping track of the supply of drugs, from manufacture to the patient's receiving it. It will certainly be a key player in the pharmaceutical sector of the

healthcare industry by minimizing fraud and managing the counterfeiting of drugs. Forging, and fraudulent activities concerning medication, have become a problem for the industry. They are plagued by financial losses in the sector, and have a defined negative impact on the health of patients. With the help of blockchain technology, it is possible to rely on the tracking of pharmaceutical products. The details are securely stored in a digital distributed ledger, which renders a mean to mark the overall procedure of medicinal transactions against, during their complete lifecycle. The decentralized and immutable nature of blockchain technology is expected to mitigate the challenges faced by counterfeiting. Since there is no third party dealing with the drug supply, it will responsively reduce the vulnerability of mediators to be bribed. The anti-tampering potential of this elusive technology will certainly put a halt on such alarming incidents, which susceptible to introducing complexities in the healthcare society. It will then become easier for a consumer to know the pertinent information about the quality, components, and provenance of the medicines procured by the provider.

iv. **Self-regulating health claim settlements –** Health insurance is used to secure escalating costs, if by any chance, an individual encounters a medical emergency, any major accident, or the need to medicate a serious disease, and to assure that care is given when required. This insurance allows the patient to pay a part of the whole amount, with the rest to be paid by the insurer after official health claim adjudication. In this process, the cost detail is forwarded to the insurer as a claim, and the care coordinators are finally paid directly by the insurer, since it is their sole responsibility to take care of the financial aid needed by the patient. But a minor error in this process may lead to cancellation of the claim, or may lessen the amount of the claim to be paid. If no error occurs, the claim will be paid in full by the insurer. The adjudication to either pay in full, or decrease the amount, is taken by the insurer, depending on the billing procedure after identifying whether it is as required for the treatment, or unfit for it, as per the conventional codes of procedure. [15] Though in the current area of health claim settlement, a large number of claims are automatically processed in spite of the anticipation of confronting errors and frauds in the claiming procedure. Thus, it is significant to code the claims precisely, to avoid such errors becoming a hindrance in the

payment of the claiming process, since a single fault in the spelling of the patient's name may negate the application submitted. Bringing the context of blockchain technology into light, it is believed that automatic claim settlement will eventually be an easy task. The smart contracts involved in it offer a remarkable opportunity for the care coordinators and the insurer. by creating a trust-based, transparent environment. These further aid in eliminating or verifying the potential chances of frauds and error, scrutinized in a considerably more timely way.

v. **Interchange of patient data records –** As stated in the official website of the National Coordinator for Health Information Technology (ONC)**, "**An electronic health record (EHR) is a digital version of a patient's paper chart. EHRs are real-time, patient-centered records that make information available instantly and securely to authorized users." The pressing issue relating to EHR today is that it faces the major challenge of ensuring security and data integrity by preserving the data privacy of the patient. Moreover, the present EHR system significantly encounters the problem of assuring who recorded what, and when, in the EHR. This makes it nearly impossible to develop or create a trust-based environment for decision-making. Along with this, several questions on the current EHR system have been raised. The questions were on how to solve the pertaining issues involved with the multiple viewers of data, while continuing with a reliable contemporary history of all the services, medications, and treatments, provided to the patient. Reckoning the concept of EHR, the healthcare society is preparing to bring the electronic health record system under the complete influence of blockchain technology. This is being done to assure the maintenance of a distributed and secured health record system, which gives the sole authority to the patient to control the viewers of his/her data. This will enable the healthcare coordinators to provide the right treatment accordingly. Thus, the deployment of blockchain technology in the EHR will enable cost effectiveness and interoperability. It will allow an efficient and agreement-based exchange of data between healthcare providers and patients, improving the quality of data. It will also minimize the time needed to access the data at any point of service. This mitigates the need for particular software to gain access to the patient's data in EHR.

This will simplify the evolution of health data, and remove the need for any appointed intermediary.

vi. **Tracking of medical device data –** The adoption of medical devices with the help of the internet of things is drastically changing the life of every human being. It has become very easy for everyone to stay connected and updated in every second of life. Moreover, over the next few years, it is supposed to bring radical change in the relationship between humans and machines. In this regard, blockchain will help in securing these data, and, due to its decentralized feature, the communication between the patient and the healthcare provider will be more transparent. Since blockchain allows the patient to control the viewers, it will assist the care coordinator in promptly advising the patient in case of emergency, through tracking the data of these devices. [12] The remote tracking of medical device data allows the patient and the permitted providers to coordinate with each other, and keep a note of every update of his/her health information. In addition, blockchain will also help in protecting the privacy of the patient's health data through cryptography. It will secure the integrity of the data if any medical device or wearable technology is lost.

vii. **Opioid prescription tracking –** In the present context of the US**,** there is an outbreak of prescribing opioids for diagnosis, which is now a matter of severe concern. The prevailing prescription tracking system is not used appropriately for immediate action to be taken. Thus, including blockchain technology in prescription tracking may result in avoiding the complexities of over-prescription and data hoarding. [29] The decentralization and audit trailing properties of blockchain technology will enhance the beauty of the prescription tracking system by making prescriptions safer, and adding up incentives for prescribing fewer medicines. Nowadays, healthcare coordinators and pharmacies are encouraged to provide opioids to patients for the relief of pain or physical therapy, but this intake subsequently leads to addiction, rather than complete relief. Keeping this in mind, an exact and proper technical solution is required to reform these initiatives. With respect to this reformation, a blockchain technology-based system can contribute to establishing a trustworthy environment for the wise transaction of opioids, by tracking whether or not they are high in amount in comparison to the diagnosed need. This will incentivize patients to

be alert, and allow them to receive genuine treatment from healthcare providers, keeping them safe and sound from any additional risk of addiction.

viii. **Digital identity of patient –** The identity of the patient is a basic element of a health information exchange which looks for the patient in a healthcare database, using a set of unique data. The mismatching of identities has led to duplication of records, as well as access to improper medical information. [14] There is a hidden cost associated with this, when the need for a mediator to rectify such wrong information in the database arises. This may further become a hindrance during claim adjudication, and with this, the data may be vulnerable to theft, as personal information is open for all. Blockchain technology ensures the provision of a functional, unified, identity management system. It secures the personal identity of a patient by encrypting all the data, and providing a unique address to each of the patients, creating a universal patient profile to be used in widely national and international regions.

ix. **Medical research –** The authenticity of the ostensible blockchain technology has made it possible for health researchers to use real-time health data of a patient for further research work, and make it available to the field, securing the patient's identity by protecting his or her privacy of the data provided. The patient may even earn, by getting incentives for sharing his/her data, with the motive of contributing to clinical research, assuring the patient can feel protected about ensuring that there is no possible chance of encountering data theft. Such a platform will give rise to a better understanding of real world health data, because direct access to the vast storehouse of integrated real clinical data.

3. Challenges and Limitations of Blockchain Technology

As every path has its puddle, similarly every emerging technology has both its advantages and disadvantages. Any technology needs to face some challenges, as well as risks, on the path leading eventually towards higher levels of its execution. There are a number of organizational and technological challenges which limit the use of blockchain technology in the healthcare sector. [17] The hurdles on the way to achieve thorough advancement in this nascent technology are as follows:

i. **Inconsistency:** A situation which is supposed to arise in the near future is inconsistency. This is because there are not many real-life applications of blockchain available which can work as an influential example for the developing blockchain applications. The era of blockchain technology is about to unfold various new implementations which will extensively disrupt the healthcare industry. But as we do not know how perfectly the execution of these applications will take place, this leads to uncertainty.

ii. **Storage capability:** Blockchain technology will be holding thousands of data if it is applied in the area of healthcare. Healthcare information may consist of several medical images, lab reports, prescriptions, schedule tables, and significant documents, which will need more storage than the existing record system. Moreover, all the users of the blockchain system will have a copy of the data, which will eventually create the need to increase the storage capacity. Otherwise, this will give rise to significant problematic issues.

iii. **Ownership of the data:** The reason behind the dilemma of who owns the data, or who is going to be the central authority, is as yet undecided. [28] Basically, the need to have such structural or organizational infrastructure of the blockchain system is important. As this trust environment promises to be provided with blockchain architecture, it will need a self-regulating, secure department, which is not yet developed, or planned.

iv. **Cost:** The expenses regarding the use of its applications are still uncertain. Most importantly the establishment and maintenance cost of the healthcare blockchain is still unknown. Thus, it is considered to be one of the major challenges blockchain-based healthcare is about to encounter in implementing the relevant applications.

v. **Code and conduct of the administrating body:** There are no certain policies or acts present in the current world for regulating the sheer volume of the forthcoming crisis of blockchain in healthcare. There is an urgent need for a regulating body which voluntarily works for the adaptation of vital policies for the appropriate use of blockchain-based healthcare systems.

vi. **Changing the norms:** The traditional methods currently used by many doctors are still paper-based, and thus it will become hard for them to suddenly change their ways of prescribing and recording health data. Changing or updating technology itself is not hard, since it is already developed, but the variation in the customary involvement with this technology is intense. This will play a major role, as a serious challenge which needs to be handled in the future, because it deals with the mentality of every human being, or healthcare provider, involved in it.

vii. **Implementing a distributed ledger in healthcare:** Healthcare providers and insurers are supposed to share the same ledger which records all the relevant data regarding the patient. But by any chance, if even one of them refuses to provide their respective data record, it will create a huge trouble for everyone sharing the ledger. As it will not allow other users to take wise decisions depending on the records given, this will result in a severe outbreak of patients' declining the usefulness of a blockchain healthcare system.

viii. **Security breaches:** The patient will have the private key of the blockchain system. Whenever a care provider wants to have an entry in the database, the patient will need to permit him/her access to the system. But it may happen, that the patient is unable to keep a watch on the regular updating activities of the ledger. Then he/she will need someone who can help to solve certain issues on time. This will promote sharing of the private key with that chosen representative. This will somehow give rise to a situation where the security, or the main purpose of the 'security' feature is hampered.

4. Risks of Blockchain Technology

Cybersecurity has been a matter of concern ever since the evolution of the internet, but this is increasingly being considered as a vital issue after blockchain technology has come to light. As per the dictionary meaning of cybersecurity, it is "the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this." The security features underneath blockchain technology might restrict intruders' intention to interrupt, but do not make it absolutely immune to all attacks; at times blockchain might be more risky than the usual databases.

The security vulnerabilities held at the terminal points of blockchain may play a major role in the increase of security threats. These are the main causes of interoperability between humans and blockchains. This gateway usually allows inputting of data, and also outputting the processed data, as and when needed. It is necessary to secure these points, as this is when the possibility of attack increases. The main concern here is the exposure of the credentials which can weaken the strength of the security at the time of accessing the digital shared ledger.

Smart contracts are a basic need of blockchain technology, and it is important to design them accurately to make them able to prevent any sort of disruption in the structure of the consensus. Moreover, the lack of standards and regulations on using blockchain technology will lead to several unwanted issues. These might not get resolved, which in the long run may contribute to corruption of the data held in the ledger.

5. Future Predictions for Blockchain Technology

It is expected that the use cases of blockchain will take a revolutionary turn towards the healthcare system even more than expected. 2019 will play a leading role in bringing about these changes in the sector of the healthcare ecosystem. The prevailing imbalance between the issues of scalability, security, and decentralization in blockchain technology are expected to be resolved easily. These three issues have been the constant barriers in the development of the highly appreciated technology of blockchain. Much work has already been done to bring out solutions for these problems, but the work is yet to be completed. This will allow easier transactions without any interference. This will also preserve the underpinning features of blockchain technology; security and decentralization. It will rapidly increase the chances of developers in building much-needed applications for blockchain-based real-life systems. The use cases of blockchain technology do not only rely on the healthcare ecosystem for 2019, but have also expanded their reach beyond dealing with cryptocurrencies. The blockchain society is now concentrating on where its real-life application will genuinely fit the purpose, rather than being in a dilemma as to whether or not it will fit the purposes of application. There are various upcoming ideas relating to blockchain which will increase the visibility of the real-world applications in the coming days. There is expected to be considerable investment in the field of blockchain technology in 2019, and onwards, for entering a new age of development in various arenas. Decentralized apps (dAPPS) are expected

to be developed in huge numbers, which will certainly have millions and billions of users on any single day of a year. Blockchain teams are planning to explore its real life applications, and disrupt several industries, to bring about growth in the field of blockchain in various aspects. Artificial intelligence and the internet of things are now ongoing trends which have complete focus on making life easier, and are applicable for all related industries. The prime focus now is on the amalgamation of blockchain with the internet of things and artificial intelligence, which will certainly bring about major change in the way things are dealt with in every personal and professional area. This usability will rapidly increase the advances in every industry dealing with blockchain, allowing users to have the best of this tri-combination. All these expected developments need an increasing number of members in their teams, who can help in improving more and more facilities for their industries. For this particular target, we need to grow educational facilities for blockchain developers. This will eventually allow, and help them to move forward, with the aim of exploring this field in various industries, and bringing about revolutionary change in the use cases of blockchain.

6. Conclusion

Blockchain technology is an innovative technology, and the plan to implement it in the healthcare sector is expected to be the best technological advancement in the present world, by far. It has the ability to bring about a drastic change in the digital healthcare records system, by accumulating various users, such as doctors, pharmacists, healthcare helpers, caretakers, etc., in the same arena, providing a better and more appropriate decision-based treatment to the patient. Blockchain is expected to bring about a tremendous revolution in the healthcare industry, by offering a decentralized, secure, and immutable digital health record. It will gradually decrease the need for any human intervention, as well as reducing the extra costs associated with connected third parties. The complete reliability of this technology is still at risk, as it is not practically implemented in every way in a vast arena such as the health industry. The interoperability feature of blockchain will serve as the smartest use case for the healthcare ecosystem, as it will deliver the fastest opportunity to be inter-connected. This newest innovation will also aid in medical field research, enabling every medical researcher to get the most out of it. Nevertheless, since it is an emerging technology, it is anticipated that it will introduce a completely new healthcare system to the world in the near future. This will serve the purpose of an internationally accessible system,

giving patients and healthcare providers the opportunity to communicate more easily, whenever any of them is in urgent need of connecting with each other.

References

[1] Matthias Mettler M.A. HSG, "Blockchain Technology in Health Care-The Revolution Starts Here", IEEE 2016.
[2] Suveen Angraal, Harlan M. Krumholz, Wade L. Schulz, "Cardiovascular Perspective: Blockchain Technology, Applications in Health Care", 2018.
[3] Ming Chao WONGa, Kwang Chien YEE and Christian N HR, "Socio-Technical Considerations for the use of Blockchain Technology in Healthcare", 2018 EFMI.
[4] Tsung-Ting Kuo,1 Hyeon-Eui Kim,1 and Lucila Ohno-Machado, "Blockchain Distributed Ledger Technologies for Biomedical and Healthcare applications", AMIA 2018.
[5] Mark A. Engelhardt, "Hitching Health Care to the Chain: An introduction to Blockchain Technology in the Health Care Sector", TIMR 2017.
[6] James Brogana, Immanuel Baskaranb, Navin Ramachandran, "Authenticating Health Activity Data using Database Ledger Technology", Elsevier CBS Journal 2018.
[7] Peng Zhang, Douglas C. Schimidt and Julies White, Gunther Lenz, "Blockchain Technology Use Cases in Healthcare."
[8] Citrus Tech, White paper, "Blockchain for healthcare", May 2018.
[19] Mike Myburg, "Applying Blockchain to the Healthcare Industry", TIBCO.
[20] A comprehensive strategy guide, "Reinventing healthcare: Towards a global, blockchain-based precision medicine ecosystem."
[21] Grant Thorntorn, "A beginner's guide to blockchain".
[22] David Randall. Pradeep Goel and Ramzi Abujamra, "Blockchain Applications and Use Cases in Health Information technology".
[23] Neil Pithadia, Focus paper, "Understanding Blockchain: Opportunities in Healthcare".
[24] Capgemini, "Blockchain; A Healthcare Industry View"
[25] Liam Bell, William J Buchanan, Jonathan Cameron and Owen Lo, "Applications of Blockchain Within Healthcare".
[26] Chet Stagnaro, White Paper: "Innovative Blockchain uses in Health Care".

[27] Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research
[28] Blockchain distributed ledger technologies for biomedical and health care applications, *Journal of the American Medical Informatics Association*, Volume 24, Issue 6, November
[29] How to Use Blockchain for Diabetes Health Care Data and Access Management: An Operational Concept.

Authors Bibliography

Shahrin Sadik is pursuing Masters at International Islamic University of Chittagong (IIUC) in Bangladesh. Her research interests include blockchain, health care and security.

Mohiuddin Ahmed attained his PhD in Computer Science from UNSW Australia. His research expertise encompasses cyber security and machine learning, and covers a wide range of application domains. Mohiuddin holds over five years of data science and cyber security experience. He is currently working as a Lecturer in Computing and Security Sciences in the School of Science at Edith Cowan University. Prior to joining ECU, he served as a Lecturer in the Centre for Cyber Security and Games at Canberra Institute of Technology (CIT) and was also involved with CIT's Data Strategy Working Group.

Md Hasan Furhad is working as a Lecturer for the Centre for Cyber Security and Games at Canberra Institute of Technology (CIT), REID Canberra. His research interests include, cyber security, blockchain, e-commerce, web security vulnerabilities. Prior joining to CIT, he completed his PhD from University of New South Wales, Australia in the field of Computational Image Processing. Prior to that he has completed Master by Research from University of Ulsan, South Korea in the field of Embedded Computer Architecture.