BLOCKCHAIN APPLICATIONS IN CYBERSECURITY SOLUTIONS

Editors:

R. Agrawal

N. Gupta

Bentham Books

Blockchain Applications in Cybersecurity Solutions

Edited By

R. Agrawal
Faculty of Computer Applications
Manav Rachna International Institute of Research and Studies
Faridabad
India

&

N. Gupta
Faculty of Computer Applications
Manav Rachna International Institute of Research and Studies
Faridabad
India

Blockchain Applications in Cybersecurity Solutions

Editors: R.Agrawal and N.Gupta

ISBN (Online): 978-981-5080-59-9

ISBN (Print): 978-981-5080-60-5

ISBN (Paperback): 978-981-5080-61-2

Published by Bentham Science Publishers Pte. Ltd. Singapore. All Rights Reserved.

First published in 2023.

BENTHAM SCIENCE PUBLISHERS LTD.

End User License Agreement (for non-institutional, personal use)

This is an agreement between you and Bentham Science Publishers Ltd. Please read this License Agreement carefully before using the ebook/echapter/ejournal (**“Work”**). Your use of the Work constitutes your agreement to the terms and conditions set forth in this License Agreement. If you do not agree to these terms and conditions then you should not use the Work.

Bentham Science Publishers agrees to grant you a non-exclusive, non-transferable limited license to use the Work subject to and in accordance with the following terms and conditions. This License Agreement is for non-library, personal use only. For a library / institutional / multi user license in respect of the Work, please contact: permission@benthamscience.net.

Usage Rules:

1. All rights reserved: The Work is the subject of copyright and Bentham Science Publishers either owns the Work (and the copyright in it) or is licensed to distribute the Work. You shall not copy, reproduce, modify, remove, delete, augment, add to, publish, transmit, sell, resell, create derivative works from, or in any way exploit the Work or make the Work available for others to do any of the same, in any form or by any means, in whole or in part, in each case without the prior written permission of Bentham Science Publishers, unless stated otherwise in this License Agreement.
2. You may download a copy of the Work on one occasion to one personal computer (including tablet, laptop, desktop, or other such devices). You may make one back-up copy of the Work to avoid losing it.
3. The unauthorised use or distribution of copyrighted or other proprietary content is illegal and could subject you to liability for substantial money damages. You will be liable for any damage resulting from your misuse of the Work or any violation of this License Agreement, including any infringement by you of copyrights or proprietary rights.

Disclaimer:

Bentham Science Publishers does not guarantee that the information in the Work is error-free, or warrant that it will meet your requirements or that access to the Work will be uninterrupted or error-free. The Work is provided "as is" without warranty of any kind, either express or implied or statutory, including, without limitation, implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the results and performance of the Work is assumed by you. No responsibility is assumed by Bentham Science Publishers, its staff, editors and/or authors for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products instruction, advertisements or ideas contained in the Work.

Limitation of Liability:

In no event will Bentham Science Publishers, its staff, editors and/or authors, be liable for any damages, including, without limitation, special, incidental and/or consequential damages and/or damages for lost data and/or profits arising out of (whether directly or indirectly) the use or inability to use the Work. The entire liability of Bentham Science Publishers shall be limited to the amount actually paid by you for the Work.

General:

1. Any dispute or claim arising out of or in connection with this License Agreement or the Work (including non-contractual disputes or claims) will be governed by and construed in accordance with the laws of Singapore. Each party agrees that the courts of the state of Singapore shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this License Agreement or the Work (including non-contractual disputes or claims).
2. Your rights under this License Agreement will automatically terminate without notice and without the

Bentham Science Publishers Pte. Ltd.
80 Robinson Road #02-00
Singapore 068898
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

FOREWORD

Currently, there is an increase in the number of social media platforms that we use, and most of them have so-called weak and unreliable passwords. During social media interactions, large quantities of metadata are collected, and hackers can take advantage of this and create havoc. In contrast to end-to-end encryption, blockchain technology can be used to develop a standard security protocol. As part of a unified API framework, it can also be used to enable cross-messaging capabilities by securing private messaging.

Even though the blockchain is not infallible, it has evolved to become one of the most foolproof means of transacting in the world of digital networks. Since the technology is designed and intended to ensure information integrity, it has been praised for its effectiveness. There are many sectors that can benefit from it if it is used properly. As blockchain has the potential to be practical for many utilisations, it can be implemented for many uses in a variety of ways. The most practical use of this kind of system would be to use its integrity assurance to build cybersecurity solutions for many other technologies as well. This book is a good step in that direction.

The book "**Applications of Blockchain in Cybersecurity Solutions,**" edited by Dr. Rashmi Agrawal and Dr. Neha Gupta, is a comprehensive book on Blockchain Technologies. The authors have tried their best to present the concepts and techniques to every extent. Practical applications of blockchain in cybersecurity are also well presented in some chapters.

Abhishek Kumar
Associate Professor
Chitkara University,
India

PREFACE

The concept of a blockchain can be defined as a linked set of records maintained in a decentralized environment. The records in the blockchain are publicly accessible but cryptographically protected. An interesting property of the blockchain is that once some information has been recorded, it is impossible to alter the information after it was recorded. An example of a blockchain can be seen as a chain of blocks containing time-stamped digital documents in such a way that they cannot be backdated or modified in any way. The time-stamped digital documents are kept as a collection of records and are grouped into a set of blocks, which are chronologically linked by date and time.

Each time the blockchain needs to be updated; a new block is created and appended to the existing blockchain. Each block in the blockchain contains a hash of the previous block, a collection of records of its own, and the hashed value records, also known as Merkle trees, that correspond to the block before it. Depending on the nature of the blockchain, the information inside each block differs. For instance, when it comes to bitcoin, the blockchain is supposed to store the complete details about a transaction, namely the sender, the receiver and the number of coins, whereas a blockchain used for medical records is supposed to store the complete health history of a patient over time. As blockchains are distributed, efficient hashing techniques are used to ensure their integrity and robustness. Eleven chapters of this book are devoted to demonstrating the benefits and applications of blockchain.

“Introduction to Blockchain Technology”, in the first chapter, briefly explains what blockchain technology is all about. The chapter focuses on the nuances of blockchain technology, the protocol stack, and the most common consensus mechanisms used. Additionally, recent advances, challenges, and future trends of blockchain are discussed in this chapter.

The second chapter discusses the relationship between cybersecurity and blockchain. Blockchain technology plays a crucial role in strengthening cybersecurity in various industries due to its decentralized nature. Through this chapter, the readers will get to know how blockchain technology is helping in providing cybersecurity to the different sectors of industries with its advantages and disadvantages of blockchain. The author also explores the role of blockchain in cybersecurity and the future benefits of blockchain technology to strengthen cybersecurity.

A majority of specialists are working on the acceptance of blockchain to safeguard IoT (Internet of Things) devices, systems, and information. Chapter 3 will examine the methods proposed by previous analysts through which blockchain can carry the expense of security. The chapter will illustrate the subjective investigation of supporting information to assess the relevance of Blockchain innovation in the present cybersecurity industry.

Chapter 4 is on “Attack Surfaces in Blockchain”. Attacks are believed to be caused by the blockchain cryptographic architecture, the bottom-line architecture, and the substance in which they are applied. Progressive defense research is believed to be the primary threat. Current research suggests that other attacks on the blockchain can be launched without being able to withstand traditional defenses, a few of which may be used to deliver other attacks. Delineating these attacks and examining their countermeasures reveal the direction of new research that should be pursued to foster safer and more competent use of blockchains.

Blockchain technology offers a data format that has built-in security. It is built on cryptography, decentralisation, and consensus concepts to ensure trust in transactions. Decentralization is enabled by blockchain technology, which allows members to participate in a distributed network. Since all transactions are transparent and visible to all users on the network, a single user cannot alter the transaction. However, blockchain differs significantly from other systems in terms of security. The blockchain is vulnerable to so many attacks nowadays. The purpose of Chapter 5, "Review of Anti Counterfeit Solutions in Block Chains", is to examine the effective anti-counterfeit measures taken by blockchain technology or the patches for and related vulnerabilities offered by researchers to reduce the impact of these attacks.

Due to the increasing number of connections, the popularity of cloud services, and advances in the Internet of Things (IoT), a decentralized approach to trust is becoming more common. In the research community, blockchain technology is receiving considerable attention because it provides a distributed ledger. This technology, however, does not provide cybersecurity in its entirety. Thus, the objective of this chapter is to provide a comprehensive overview of the proposed methods and factors for achieving cybersecurity in blockchain-based systems.

The objective of the Sixth chapter, "Preserving the Privacy of Wearable IoT Device Data Using Blockchain," is to provide the solution for the above-mentioned problems using Blockchain technology.

The cloud environment is a way to use faraway servers accommodated on the internet for data storage, data control, and information processing, more readily than a private computer or native server. There are still many challenges in the cloud environment, including authenticity, confidentiality, and integrity.

Chapter 7 discusses Blockchain-Based Access Control Systems. The need for secure and distributed access control architecture to overcome the single point of failure problem of a centralized entity becomes a big challenge when coupled with scalability and lightweight features. It is possible to achieve this through the use of Blockchain technology, which has recently been used to provide access control services. IoT device management would be used to manage distribution, heterogeneity, scalability, the ability to tolerate failure, security and privacy aspects of IoT devices at scale in the near future as it is useful.

"Multi-chain Deployment over Smart Contracts" is covered in Chapter 8. As the greatest enabling technology for blockchains, smart contracts are considered to be the best. As a result, blockchain ecosystems become self-governing, transparent, consent-based, and credible. Blockchains can operate without human intervention due to a compilation of smart contracts. These smart contracts are set up so they can be deployed at the predefined blockchain nodes. This can be done through the callbacks either from the blockchain system, the other smart contracts, or even the participants' information systems. As smart contracts, both the operations on the blockchain and the rules that govern the applications can usually be predetermined. While the use cases and real-world functions of this technology differ from one another, some principles remain the same: immutability, transparency, redundancy, and security.

The title of Chapter 9 is "Blockchain for Decentralized Services: On Improving Security and Performance of Distributed IPFS-based Web Applications". Blockchain technology, with its associated decentralization, is used to develop decentralized application platforms. The Interplanetary File System (IPFS) is built on top of a distributed system consisting of a group of nodes that shares the data and takes advantage of blockchain to permanently store the data. The IPFS is very useful in transferring remote data. This work focuses on applying blockchain technology to the IPFS to improve its security and performance

R. Agrawal
Manav Rachna International Institute of Research & Studies,
Faridabad
India

&

N. Gupta
Manav Rachna International Institute of Research & Studies
Faridabad
India

List of Contributors

AR.G. Gokul	Department of Information Technology, Sri Venkateswara College of Engineering, Sriperumbudu, India
B.K.P. Madavi	GITAM University, Bangalore
D. Mantri	Sinhgad Institute of Engineering, Lonavala, Pune
G. Thahniyath	Dayananda Sagar University, Bangalore
H. Saini	Research Schola, IBM, GLA University, Mathura, Uttar Pradesh, India
H. Bhatia	School of Computer Scienc, Engineering and Applications, D Y Patil International University, Pune, India
I. Chatterjee	Department of Computer Engineering, Tongmyong University, Busan, South Korea
K.K. Sowjanya	CMR Institute of Technology, Bangalore
M. Moh	San Jose State University, San Jose, CA 95192-0249, USA
N. Devi	Department of Information Technology, Sri Venkateswara College of Engineering, Sriperumbudu, India
N. Gupta	Manav Rachna International Institute of Research and Studies, Faridabad, Haryana
P.L. Rani	Department of Information Technology, Sri Venkateswara College of Engineering, Sriperumbudu, India
R. Agrawal	Manav Rachna International Institute of Research and Studies, Faridabad, Haryana
R. Deshmukh	Department of Computer Scienc, Shivaji University, Kolhapur, India
R. Kamat	Department of Computer Scienc, Shivaji University, Kolhapur, India
R. Moazeni	San Jose State University, San Jose, CA 95192-0249, USA
S. Zalte	Department of Computer Science, Shivaji University, Kolhapur, India
V. Garg	Amity UniversityUttar Pradesh, India
V. Le	San Jose State University, San Jose, CA 95192-0249, USA

CHAPTER 1

Introduction to Blockchain Technology

N. Devi[1,*], **P.L. Rani**[1] and **A.R.G. Gokul**[1]

[1] *Department of Information Technology, Sri Venkateswara College of Engineering, Sriperumbudur, India*

Abstract: A blockchain is a linked set of records maintained in a decentralized environment. The records in blockchain are publicly available but cryptographically secured. The interesting property exhibited by blockchain is that once some information is recorded, it is infeasible to modify the information. Blockchain is generated as a chain of blocks that contains time-stamped digital documents so that it is infeasible to back date them or tamper the documents. These time-stamped digital documents are stored as a collection of records and grouped as a set of blocks, chronologically linked in order of time.

A new block is created and appended to the existing blockchain, whenever there is a need for updating the blockchain. Every block in the blockchain comprises of a hash of the preceding block, collections of records of its own, and the hashed value records known as merkle tree. The information inside the blocks varies depending on the nature of blockchain. For example, when the nature of blockchain is bitcoin, they are supposed to store the details about a transaction *viz.*, sender, receiver and amount of coins where as blockchain used for medical records stores the complete health history of a patient over time. Since blockchain is stored in a distributed way, efficient hashing techniques are used to ensure the integrity and robustness of blockchain. This chapter describes the nuances of blockchain technology along with the protocol stack and the most common consensus mechanisms. Furthermore, recent advances, challenges and future trends of blockchain are discussed.

Keywords: Bitcoin, Blockchain, Cryptography, Distributed, Decentralized, Hash, Merkle Tree, Robustness, Time Stamp, Transaction.

INTRODUCTION

A blockchain [1] is a decentralized distributed ledger of records that is cryptographically secured and accessible unlimitedly to all. It possesses a fascinating characteristic: when an information is stored inside a blockchain, it is infeasible to modify the recorded information. The blockchain is generated as a

[*] **Corresponding author N. Devi:** Sri Venkateswara College of Engineering, Pennalur, Sriperumbudur, Kancheepuram, Tamil Nadu, India; E-mail: leela@svce.ac.in

Rashmi Agrawal and Neha Gupta (Eds.)

chain of blocks that contains time-stamped digital documents.. These time-stamped digital documents are stored as a collection of records and grouped as a set of blocks. These blocks are then linked together in chronological order of time in a continuous line. To update, a new block is created and appended to the existing blockchain, thus, providing blockchain, a non-destructive way to track data changes over time. Every block in the blockchain comprises hash of the preceding block, collections of records of its own, and the hashed value records known as Merkle tree. The information stored inside the blockchain depends on the type of blockchain. For example, the blockchain used in bitcoin records the information of a transaction *viz.*, number of coins, contributor and receiver whereas the blockchain used for medical records stores the complete health history of a patient over time. Since blockchain is stored in a distributed way, efficient hashing techniques are used to ensure the integrity and robustness of the blockchain. The main characteristics of blockchain are depicted in Fig. (**1**). This section describes the nuances of blockchain technology.

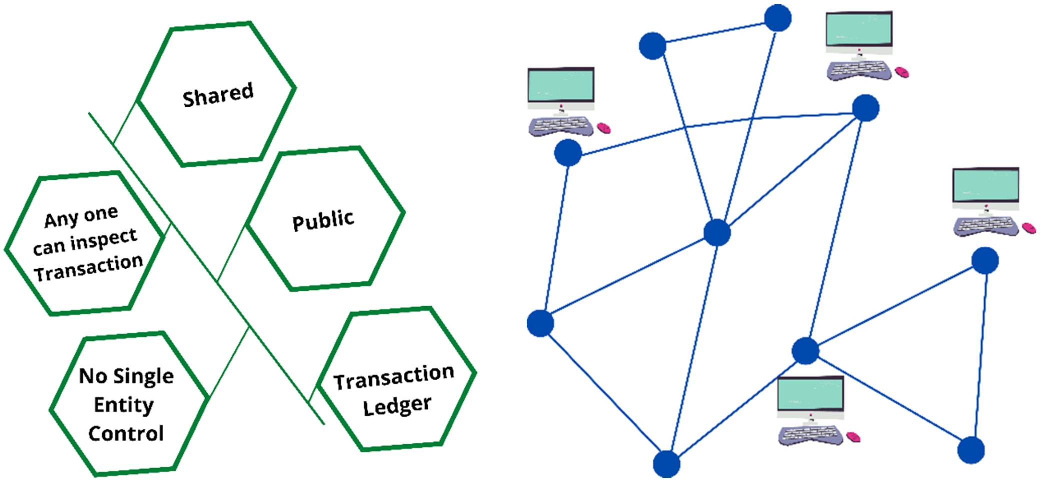

Fig. (1). Different Aspects of Blockchain.

Block

A block in a blockchain is a collection of various items such as the hash of its preceding block, the Merkle root and its own records as shown in Fig. (**2**). A Merkle tree for a block is formed by placing the hash of the individual records of that block as the leaf nodes and the non-leaf nodes are the combined hash of their own children. Using hash ensures data integrity and also helps in ensuring the correctness of the data at any given time. A hash function accepts an input of any length and converts it into a fixed length. The hash function may produce a 32-bit or 64-bit or 128-bit or 256-bit fixed length called a hash. Hash functions protects the data integrity. If a trusted hash of the data is provided, it is possible to compute the hash of the data and verify the two values. If they match, then the data has not been changed since the original hash is formed.

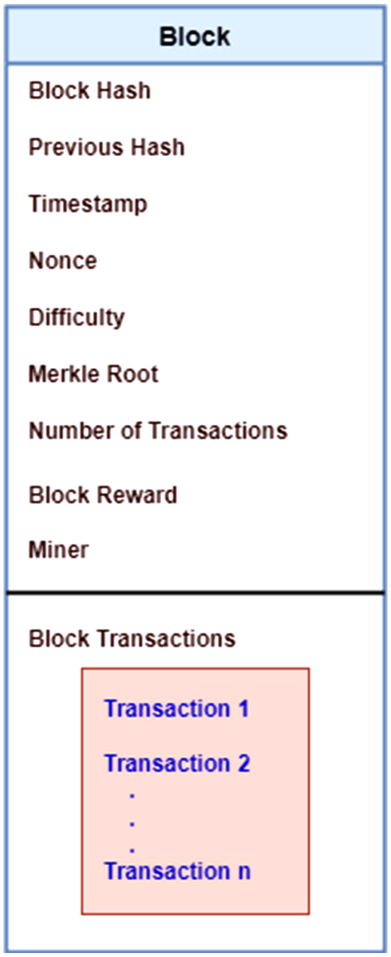

Fig. (2). Block in a Blockchain.

The first block is called a genesis block and is created at the beginning with the set of records and its Merkle root.

Merkle trees are the basic blocks of blockchain technology. It is a structure that permits verification of the consistency of content in a secure and efficient way. Bitcoin and Ethereum use Merkle trees. A Merkle tree produces a fingerprint of the summary of all the transactions in a block. It enables a user to verify whether a transaction is part of a block. Repeated hashing of pairs of nodes is performed from the bottom up, until only one hash is left as depicted in Fig. (**3**). This hash is

CHAPTER 2

Cybersecurity and Blockchain

H. Saini[1,*] and **V. Garg**[2]

[1] *Research Scholar, IBM, GLA University, Mathura, Uttar Pradesh, India*

[2] *Amity University, Uttar Pradesh, India*

Abstract: Blockchain technology provides unprecedented security to sensitive data to both businesses and individuals; it has become one of the most famous methods for securing data through a decentralized system. Cybercrime is a serious threat to enterprises as hackers are devising new techniques and implementing them to execute cybercrime. Blockchain technology has the potential to give higher security, which has no limit to keeping important and sensitive information and records. Blockchain is the technology that could go a long way in fighting this and keeping digital information safe and secured. Blockchain technology strengthens cyber security for different areas of industries and plays a vital role in making data more secure with its decentralized technology. Through this chapter, the authors will get to know how blockchain technology helps in providing cyber security to the different sectors of industries with its advantages and disadvantages of blockchain. The author also explores the role of blockchain in cybersecurity and the future benefits of blockchain technology to strengthen cybersecurity.

Keywords: Bitcoin, Blockchain, Blockchain in industries, Challenges with Blockchain, Crypto currencies, Cyber-attack, Cyber security, Data security, Decentralized, Internet of things (IoT).

INTRODUCTION

Blockchain is a database that is different from the usual database storing systems. Blockchain stores the data like a normal database system but it stores the data electronically in the form of groups in the computer system. The information saved through blockchain technology is saved in a set of groups that are also known as blocks that are later chained altogether into chronological order. Once the data is filled in the current block, new data will be stored in the new block automatically, and once data will be stored in new block, it will again be automatically added to the next block which becomes a chain of the trailing blocks. The most common use of the blockchain system is in ledger transactions.

[*] **Corresponding author H. Saini:** Research Scholar, IBM, GLA University, Mathura, Uttar Pradesh, India; E-mail: vgarg@gn.amity.edu

Rashmi Agrawal and Neha Gupta (Eds.)

This record-keeping technology also works behind the Bitcoin network. In the case of bitcoin, decentralized blockchains are used so that any individual or group cannot control it. It also keeps records of all the data permanently that can be viewed later as per the need [1].

Daily, 2020 [2] stated that blockchain's instinctively decentralized nature makes it a perfectly suitable technology for cybersecurity. Blockchain technology is used as a new weapon in cybersecurity. CEO of IBM Ginni Rometty said that to every profession, industry, and company present in the world, cybercrime is the greatest threat for them. Cybercrime is very extensive and expanding very quickly in the industries of the world.

In an article published by Consolidated Technologies Inc., it has been said that blockchain gives cybersecurity to businesses by protecting their critical and sensitive data, and can also protect cryptocurrency and other smart assets of the entrepreneurs. Blockchain keeps the information safe by tracking and checking every single change that occurs in a database, backing up the data in numerous locations, identifying and pointing out the attacks and errors, and preventing identity theft by authenticating the data and keeping hackers out [3].

The amount of data generated by industries, businesses, and individuals is increasing day by day without any end to it. To the current demand of each sector, developing more sophisticated technologies to ensure the security of the stored data and information from hackers has become mandatory to put a stop to cybercrimes. There are strong culminating points of damning that affect cybersecurity: human error-caused data breaches, malware delivered by emails, fake invoices for malware distribution, *etc.* In the future with 5G networks, superfast download speeds will encourage huge cybercrimes as the number of globally connected devices through the IoT (Internet of Things) devices will also increase to the amount to 13.8 billion devices in 2021. Here is the situation where blockchain needs to strengthen cyber security [4]. Security experts have found blockchain as a solution for increasing cybercriminals that have been continuously evolving. Blockchain applies to almost all sectors of industries but its role in cybersecurity is more transformative [5]. The popularity of blockchain has increased worldwide, and apart from being a popular technology it also has successfully made its impact on the world. And now industries across the world are grasping the new technology that gives assurance of safety to the data and security with blockchain cybersecurity technology that is now leading the way. Blockchain technology has been commercially adopted and companies are queuing up to accept the largest cryptocurrency [6]. The distinctive characteristics of blockchain technology make its application different and attractive for many business ideas such as banking and there are majorly five areas of the banking industry that are affected the most. The affected areas of banking are Clearing and Settlement, Payment, Trade Finance, Identity, and Syndicate Loans [7]. However, industries are applying the core concept of blockchain technology to their existing business processes most importantly for cybersecurity solutions, and guardtime federal is dedicatedly providing cyber-security solutions to the Department of Defence (United States), the Intelligence community of the U.S., and other departments of the U.S. government [8]. All these solutions offer confidentially and authenticated services.

Rijmenam, 2016 has stated that organizations are exploring this revolutionary technology of blockchain systems and finding how it can be beneficial for their businesses. It has also been observed that there is a possibility that blockchain will be used in almost all industries with some sort of transaction and many of them will face job losses as intermediaries' jobs will not be needed or needed a lot less. Blockchain is a technology that can give a well-built cybersecurity solution to information and data security issues and a high-level privacy protection tool for confidential information [9]. Furthermore, the protection given by multi-signature (multi-sig) or to authorize a transaction by more than one key, will improve security and privacy more efficiently.

Blockchain is a technology that is behind bitcoin also, and it is an open distributor ledger that records the data of transactions securely, permanently, and safely in a very efficient manner. Transferring the share stock used to take a week but with blockchain, it can be done in seconds. Blockchain has cut down the cost of transitions and eliminated the intermediary involvement of bankers and lawyers. It will take years to adopt blockchain technology like other internet technologies took years in their adoption [10]. Those companies that are into financial services are already doing well in adopting blockchain technology, and there is a strong possibility that it will affect all kinds of businesses and industries. Hsieh (2017) [11] stated in an article that blockchain security issues are critical in terms of cybersecurity. Before implementing it to the system, security experts need to go through and understand its impact, scope, and challenges carefully.

It has been expected that by 2027, identity theft will increase 25% and will cause a loss of 40.62 billion dollars [12]. The impact of cybercrime that results in payment fraud is depicted in Fig. (**1**). which describes the statistics of payment fraud, cybersecurity education is essential in the fight against hackers [13].

The CIA (Confidentiality, Integrity and Availability) triad model is used as a baseline and a standard for cybersecurity evaluation of any organization's cybersecurity strategy. Confidentiality, Integrity, and Availability are the trio that needs to be secured and Blockchain technology allows users to secure these three

CHAPTER 3

Applications of Blockchain in Cyber Security Industry

N. Gupta[1,*] and **R. Agrawal**[1]

[1] *Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India*

Abstract: A blockchain is a decentralized record that is used to securely transfer digital currencies, make agreements, and trade. Everyone in the system goes to the most recent duplicate of the encoded record in order to authorize another transaction. A blockchain record is a collection of all prior bitcoin exchanges. Fundamentally, it is a suitable database that keeps up with a continually developing, highly organized information structure of blocks that hold a large number of individual transactions. Blockchain innovation has seen adoption in a variety of organizations, most notably in the use of digital currency. Regardless, innovation is useful in cyberspace. This chapter examined a few application cases of Blockchain in the cybersecurity industry. A majority of specialists are working on the acceptance of blockchain to safeguard IoT (Internet of Things) devices, systems, and information. The chapter has examined the methods proposed by previous analysts through which blockchain can carry the expense of security. Finally, the chapter has proposed the future of a single blockchain for building cyber security applications for coordination and consistency among security arrangements.

Keywords: Bitcoin, Blockchain technology, Cyber security.

INTRODUCTION

Blockchain is a cutting-edge innovation that has the potential to revolutionize the future of processing and challenge a few businesses with more imaginative arrangements. It is open, unchanging, and adequately adapted for all intents and purposes relevant to a variety of scenarios [1]. The rise of digital currency has increased interest in the idea, although it sees uses in a variety of fields other than finance. A blockchain is roughly equivalent to a few cryptographically attached blocks. A square alludes to a three-part information structure: information, the hash of the previous square, and the hash of the information and past hash. As a result, there is a demand for trust between blocks that can be used to ensure the integrity of the entire Blockchain. If the information in any of the blocks changes,

[*] **Corresponding author N. Gupta:** Manav Rachna International Institute of Research & Studies, Faridabad, Haryana, India; E-mail: neha.fca@mriu.edu.in

Rashmi Agrawal and Neha Gupta (Eds.)

the hash value will change as well [2]. This will result in a spiraling impact in which the hashes of the resulting blocks will become invalid. This is why blockchain transactions are immutable. This foundation can be extremely useful in providing cyber security solutions in high-risk areas such as IoT gadgets, systems, and data storage and transmission.

Objectives of the Study

- To study the role of Blockchain in Cyber security.
- To study the future of Cyber security through Blockchain Technology.

Research Methodology

The chapter will illustrate the subjective investigation of supporting information to assess the relevance of blockchain innovation in the present cyber-security industry. It will concentrate on a recent report provided by Taylor *et al.* [18] that investigated 30 ongoing examinations contemplating on blockchain cyber security use cases.

ROLE OF BLOCKCHAIN IN CYBER SECURITY

The increased reliance on the web and innovation today has resulted in new revenue streams and plans of action for organizations; yet, this has also resulted in new gaps and open doors for programmers to exploit [3]. Cybercriminals have become increasingly perplexed and are attempting to take critical information like money, health records, individually identifiable data (PII), and licensed innovation, and are relying on exceptionally advantageous systems like disrupting a business's general operations through DDoS assaults, or adapting information access through the use of cutting edge ransom ware methods [4].

Given the current state of affairs, would blockchain innovation be an aid or a hindrance to cyber security? A blockchain, which employs Distributed Ledger Technology, is fundamentally a decentralized, digital, open record of all cryptographic money dealings [5]. This may aid to improve digital security because the platform may prevent deceptive exercises through agreement components and recognize information altering based on its fundamental attributes of operational flexibility, information encryption, auditability, straightforwardness, and permanence [6].

Blockchain resolves the 'lack of confidence’ issue between counterparties at a critical level. Blockchain is a distributed database that is used in both private and open applications, as opposed to a centralized system in which all data is stored in a few extremely large databases [7]. The information pertaining to each cluster of valid trades is saved within its own block; each block is related to the block which is arranged in the situation before it and develops continuously as new data blocks are affixed.

ELIMINATING HUMAN FACTOR FROM AUTHENTICATION

Organizations can verify gadgets and clients without the requirement for a secret phrase with the assistance of blockchain innovation [8]. This disposes of human mediation from the procedure of confirmation, in this way maintaining a strategic distance from turning into a potential assault vector.

The use of a combined design and simple logins is a major drawback of standard frameworks. Regardless of how much money an organization invests in security, all of these efforts are pointless if employees and clients use passwords that are simple to steal or split. Blockchain provides reliable verification while also resolving a single point of attack. A security framework used in an organization can use a dispersed open key foundation for validating gadgets and customers with the assistance of blockchain [9]. Instead of a secret word, this security framework assigns a unique SSL endorsement to each device. Because the executives of endorsement information are finished on the blockchain, it is practically impossible for aggressors to utilize counterfeit authentications.

Decentralized Storage

Blockchain users can keep their data on their PC in their system. In this way, they can assure that the chain does not break. For example, if someone who isn't the owner of a piece of information (for example, an assailant) tries to meddle with a block, the entire framework examines every single information block to discover the one that differs from the rest [10]. If this type of block is found by the framework, it simply removes the block from the chain, marking it as fraudulent.

Blockchain is designed in such a way that there is no capacity area or focal authority. On the system, each client has a task to complete in terms of storing some or all of the blockchains [11]. Everyone in the blockchain network is responsible for verifying the information that is transmitted as well as keeping it up to ensure that existing information is not expelled and fake information is not incorporated.

Traceability

Each exchange that is uploaded to a private or open blockchain is meticulously time stamped and tagged. This means that companies can trace each trade back to a certain timeframe and locate the comparable party on the blockchain using their open location [12]. This aspect is associated with non-renunciation: the assurance

CHAPTER 4

Overview of Attack Surfaces in Blockchain

S. Zalte[1,*], **H. Bhatia**[2], **R. Deshmukh**[3], **N. Gupta**[4] and **R. Kamat**[5]

[1] *Department of Computer Science, Shivaji University, Kolhapur, India*

[2] *School of Computer Science, Engineering and Applications, D Y Patil International University, Pune, India*

[3] *Department of Computer Science, Shivaji University, Kolhapur, India*

[4] *Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India*

[5] *Department of Computer Science, Shivaji University, Kolhapur, India*

Abstract: In blockchain technology, cybercriminals exploit new attack surfaces for non-legitimate persons who wish a dissemination of fake information, encourage cyber attacks, unethical behavior, *etc.* Attacks are believed to be attributed to the blockchain cryptographic architecture, the bottom-line architecture, and the substance in which they are applied. The main threat is focused on the progressive defense research activity. It is currently believed that other attacks on the blockchain can be launched without being able to withstand traditional defenses, a few of which may be used to deliver any other attack. By delineating these attacks and examining their countermeasures, it highlights the direction of new research that should be persisted for safer and more competent use of blockchain. In spite of vulnerabilities and attacks, this technology offers key features like hashing, immutability and digital signature, which enrich the blockchain. Researchers also contributed to developing a security shield for blockchain by using an intelligent combination of these features. Basically, these features are required to achieve CIA (Confidentiality, Integrity and Authentication). The contribution of this chapter would be systematically investigating the attack surface of Blockchain technology. The attack surface is the sum of all conceivable security risk exposures. It is also the total of all known and undiscovered threats, possible vulnerabilities, and controls, including all resources. To do this, we set attack vitality on the attack surface to a variety of attacks.

Keywords: Attack surface, Block chain, CIA, Defense research activity, Vulnerabilities.

[*] **Corresponding author S. Zalte:** Department of Computer Science, Shivaji University, Kolhapur, India; E-mail: sheetal.zaltegaikwad@gmail.com

Rashmi Agrawal and Neha Gupta (Eds.)

INTRODUCTION

Blockchain technology is an open-source, decentralized ledger, based on a peer-to-peer distributed network that records immutable and encrypted transactions which are verified between two entities without the involvement of a third party. Blockchain technology is secured as it is based on the concept of cryptography and peer-to-peer networks or distributed networks. The use of cryptography in blockchain technology enables to establish trust between entities of a network *via* digital signatures, enables integrity and immutability *via* hash functions and helps in transactions that are publicly verified and un-altered. On the other hand, the peer-to-peer network in blockchain eliminates the issue of single-point-of-failure and single point-of-trust, and allows for transaction ledger verification without the need for a centralized authority [1].

Apart from this, blockchain also supports other significant features like distributed ledger, consensus, availability and smart contracts *etc.,* as shown in Table **1**. Now, Blockchain technology is accustomed by the world and is being investigated in new and forthcoming novel applications [2]. Due to its vast application possibilities, blockchain has sparked a lot of curiosity among academics and industry. Blockchain technology is being employed in different domains like cryptocurrencies [5], Ethereum-based smart contract platforms and 'Decentralized Autonomous Organizations (DAOs)' like Dash and Bitshares [3, 4, 6], health care [7], Internet of Things [8, 9], financial systems [10], Vehicular Ad-hoc Networks (VANET), and edge computing [11, 12] and many more, *etc.*.

Table 1. Features of Blockchain.

Key Features	Description
Immutability	Allows to store transactions permanently and nobody can modify transactions once entered into the system.
Transparency	All Blockchain users have access to each public address's transactions, which are safe and secure.
Peer-to-peer network	Allows the execution and verification of transactions without the use of central authority or third party
Consensus	A fault-tolerant methodology and method of establishing consensus across all Blockchain participants
Smart contract	Self – executing contract allow the transaction without third parties
Distributed ledger	A decentralized database that is accessible to multiple users to create and update single, trusted transactions across multiple locations
Anonymity	The ability of node in the network to perform transaction or exchange data without revealing its identity.

The security of the blockchain is important as its use is not only limited to cryptocurrencies and smart contracts but used in large-scale systems which are used to hold delicate or user-specific sensitive data and information. In spite of the invulnerable security functionality of Blockchain technology that brings to applications, several attacks have been launched against this technology. For example, due to the popularity and capital tied to its system, blockchain-based cryptocurrencies are exposed to multiple activities that are fraudulent. Mt. Gox, a Tokyo-based Bitcoin exchange in Japan, was hacked by two malicious attackers who stole $ 460 million in bitcoins [13]. The hackers collected data from the Bitcoin blockchain and manipulated counterfeiting transactions that led to a surge in the market price. As a result of such activities, Mt. Gox suffered severe losses and, in the end, went ruined. Furthermore, the Bitcoin blockchain is overloaded with fraudulent or spam transactions, which causes legitimate transactions to be delayed. In 2017, Bitcoin storage pools were swamped by unethical transactions, which leads locks and delays in transaction verification, increasing the Bitcoin mining fee [14]. Furthermore, in June 2016, an unknown attacker managed to withdraw US $ 50 million from “The DAO”, a decentralized autonomous organization that works on smart contracts based on blockchain or pre-programmed rules that govern the organization [15]. Bitfinex was temporarily blocked in June 2017 due to a distributed denial of service (DDoS) attack. Several Bitcoin and Ethereum (a Blockchain-based distributed computing platform) exchanges have been subjected to DDoS and DNS attacks on a regular basis, causing service outages for consumers.

A potential vulnerability in the Blockchain system could be launched in unanticipated attacks, jeopardising the system's overall security and privacy. As a result, the first step is to investigate the weaknesses in the technology that led to unethical activities. Furthermore, this research examines counterfeit solutions from a systemic perspective.

BLOCKCHAIN SECURITY ISSUES

The following are five of the most serious security concerns surrounding blockchain technology, as shown in Fig. (**1**).

Transaction Malleability

Due to the popularity and wealth invested in its system, blockchain-based cryptocurrencies are vulnerable to a variety of fraudulent operations. Mt. Gox, a Tokyo-based Bitcoin exchange, has been hacked by two people [16]. Transaction malleability is a form of attack that allows a user to alter the identification of a Bitcoin transaction prior to it being confirmed on the cryptocurrency network. This modification allows the individual to pretend that no transaction occurred. It

CHAPTER 5

Review of Anti-Counterfeit Solutions in Blockchain

H. Bhatia[1,*], **S. Zalte**[2], **I. Chatterjee**[3] and **D. Mantri**[4]

[1] *School of Computer Science, Engineering and Applications, D Y Patil International University, Pune, India*

[2] *Department of Computer Science, Shivaji University, Kolhapur, India*

[3] *Department of Computer Engineering, Tongmyong University, Busan, South Korea*

[4] *Sinhgad Institute of Engineering, Lonavala, Pune, India*

Abstract: Blockchain technology offers a data format that has built-in security. It is built on cryptography, decentralization, and consensus concepts to ensure transaction confidence. Decentralization is enabled by blockchain technology, which allows members to participate in a dispersed network. No single user can alter the transaction, as all transactions are transparent and visible to all other users on the network. However, there are some significant security differences between blockchain and other systems. Nowadays, there are so many potential attacks found on the blockchain. The contribution of this chapter would be to match the effective defence taken by blockchain technology or a patch for related vulnerabilities offered by researchers to reduce the impact of these attacks. To keep the network secure and resilient, an overview of these security solutions for various vulnerabilities and attacks helps to reduce the attack surface in the blockchain.

Keywords: Cryptographic, Decentralization, Consensus, Security, Defense, Attacks.

INTRODUCTION

Blockchain is the first type of decentralization technology with no central controlling authority and is based on secure and distributed decentralized protocols. All nodes that are part of the network are responsible to generate, add and confirm the transactions within the data blocks. Blockchain technology inherits several security qualities like decentralization, hash functions, consensus mechanism, digital signatures and smart cards, which enhance and secure blockchain technology.

[*] **Corresponding author H. Bhatia:** School of Computer Science, Engineering and Applications, D Y Patil International University, Pune, India; E-mail: heenakbhatia@gmail.com

Rashmi Agrawal and Neha Gupta (Eds.)

Blockchain technology has enormous potential for a wide range of applications and offers numerous options for diverse infrastructure. A blockchain transaction uses hash functions to secure the records, and each transaction is linked to previous transactions or records. The data integrity of transaction data is protected using hash functions. Consensus algorithms on the blockchain nodes validate transactions. Since blockchain networks operate in a decentralized manner, a single entity cannot start the transaction. Each participant has the ability to view transactions at any time. Thus, blockchains enable transparency. Digital signatures are a crucial building element of blockchains that is used to authenticate the validity of transactions. A smart contract is a self-executing set of instructions, which automates the execution of transactions without third-party involvement. Ethereum is a decentralized system for executing smart contracts.

Even with such adequate and strong significant security capabilities, blockchain is still establishing itself in the market. Blockchain technology is susceptible to a variety of attacks. Attackers exploit the vulnerability present in the blockchain. As a result, Blockchain adoption has been slower than anticipated. Hence, identifying the solutions for the main reasons for such delayed adoption becomes a critical issue. In this paper, we investigate and provide counterfeit solutions for the various blockchain security-related issues and risks associated with blockchain implementation for attacks like User wallet attacks, blockchain network attacks, transaction verification mechanism attacks, Smart contract attacks and Mining pool attacks.

COUNTERFEIT SOLUTIONS FOR ATTACK SURFACES

This section will present a summary of countermeasures against the existing attack surfaces in Blockchain.

Countermeasure against Blockchain Network Attacks

Countermeasures against Distributed Denial of Service Attack

In a recent study, countermeasures focussed on multi-field coordination to alleviate DDoS attacks. In order to detect an anomalous network flow, high detection and low false alarm rate were proposed by Cheng *et al.* [1]. The Credit Bonus Penalty Strategy (CBPS) was introduced by Yang *et al.* [2] to offer an IoT confidante environment that can successfully protect against DDoS attacks. SDNs are a significant aspect of network administration because they separate control planes and data and offer novel ways to resist DDoS attacks. Saad *et al.* [3] proposed cost-effective and age-effective remedy designs, which maximize the memory pool size for a new sort of DDoS attack that affects bitcoin systems in their memory pools underlined, which lead to a significant backlog of transaction backlogs and higher mining charges.

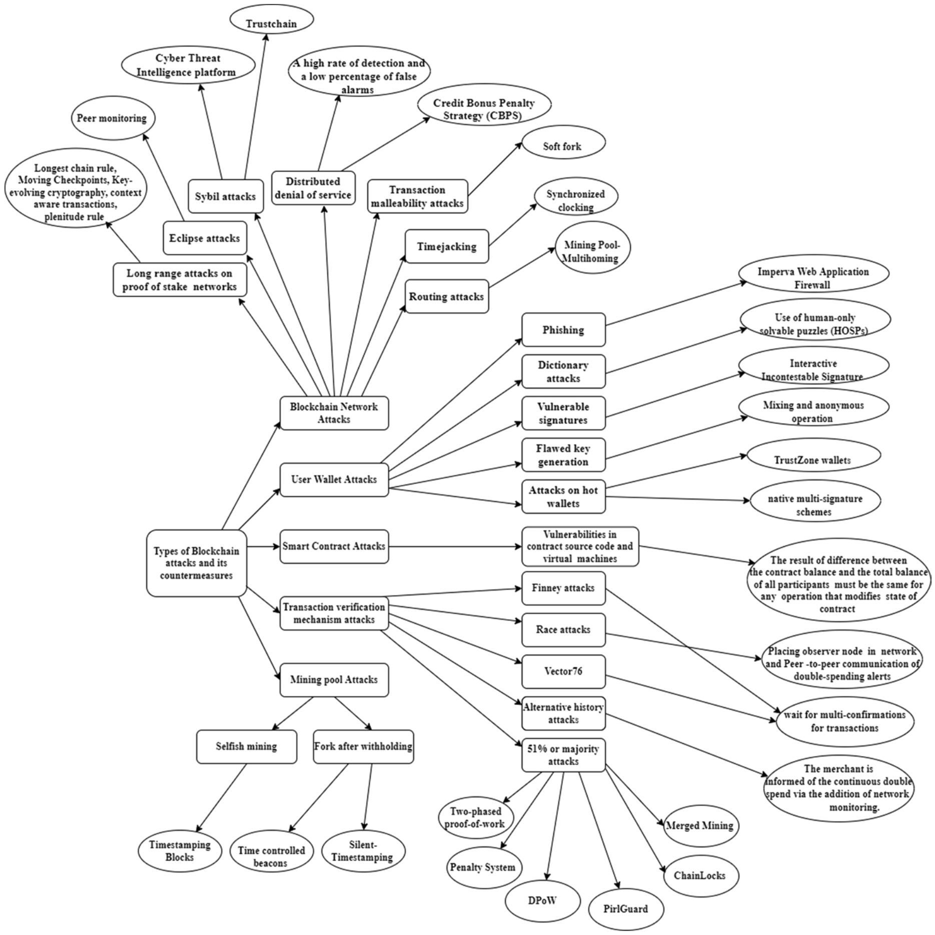
Trustchain
Cyber Threat Intelligence platform
A high rate of detection and a low percentage of false alarms
Credit Bonus Penalty Strategy (CBPS)
Peer monitoring
Soft fork
Longest chain rule, Moving Checkpoints, Key-evolving cryptography, context aware transactions, plenitude rule
Sybil attacks
Distributed denial of service
Transaction malleability attacks
Synchronized clocking
Eclipse attacks
Timejacking
Mining Pool-Multihoming
Long range attacks on proof of stake networks
Routing attacks
Imperva Web Application Firewall
Phishing
Use of human-only solvable puzzles (HOSPs)
Dictionary attacks
Interactive Incontestable Signature
Vulnerable signatures
Blockchain Network Attacks
Mixing and anonymous operation
Flawed key generation
User Wallet Attacks
TrustZone wallets
Attacks on hot wallets
native multi-signature schemes
Types of Blockchain attacks and its countermeasures
Smart Contract Attacks
Vulnerabilities in contract source code and virtual machines
The result of difference between the contract balance and the total balance of all participants must be the same for any operation that modifies state of contract
Finney attacks
Transaction verification mechanism attacks
Race attacks
Placing observer node in network and Peer -to-peer communication of double-spending alerts
Vector76
Mining pool Attacks
Alternative history attacks
wait for multi-confirmations for transactions
Selfish mining
Fork after withholding
51% or majority attacks
The merchant is informed of the continuous double spend via the addition of network monitoring.
Two-phased proof-of-work
Merged Mining
Timestamping Blocks
Time controlled beacons
Silent-Timestamping
Penalty System
ChainLocks
DPoW
PirlGuard

Fig. (1). Types of Blockchain attacks and its countermeasures. [Rounded rectangle represents type of blockchain attack and oval represent its countermeasures].

Countermeasures against Transaction Malleability Attack-

The malleability of transactions caused substantial loss and reputation damage to the community of Bitcoin. The value of Bitcoin has been decreasing since this issue, and millions of dollars in Bitcoins have been stolen. Rajput *et al.* [4] proposed a robust solution that includes a transaction Id consisting of a combination of the signature-free transaction script's hash and the ultimate transaction. This final joint hash is used for both checking and identifying the transactions. This approach is feasible and identifies any attempt at the transaction.

CHAPTER 6

Preserving the Privacy of Wearable IoT Device Data Using Blockchain

K.K. Sowjanya[1,*], K.P.B. Madavi[2] and **G. Thahniyath[3]**

[1] *CMR Institute of Technology, Bangalore, India*

[2] *GITAM University, Bangalore, India*

[3] *Dayananda Sagar University, Bangalore, India*

Abstract: Personal healthcare has become the most important part of present human life due to the COVID-19 pandemic. The awareness of one's health is made easily available by adopting IoT wearable devices like Fitbit, smart watches, oximeters, *etc.* All these devices store sensitive information like a heartbeat, BP, distance traveled, calories burnt, stress levels, location details, *etc.*, and are stored in third-party data servers. These servers are vulnerable to illegitimate users and also have a single point of failure. The personal data of the individuals should be protected along with its integrity. At the same time, the data stored in the servers should be decentralized to overcome the problem of a single point of attack. The objective of this article is to provide a framework that uses SHA-56 for generating the hash code and Blockchain technology to store the data. Thus, providing privacy, security, and integrity for the data.

Keywords: Blockchain, Fitbit, Fitbit data, Encryption, Hashing, IoT, Mining, Privacy, Security, Wearable devices.

INTRODUCTION

Smart homes, smart cities, and smart devices are driving the future generation with the help of IoT. IoT has gained so much popularity because of its heterogeneous forms and heterogeneous applications. It is changing our normal world into a digital world where interconnected devices communicate with each other through a network without human interaction [1]. Adopting this Internet of Things has introduced many technological advancements such as smart security home systems, which provide security alerts for the houses; smart agriculture systems, which provide information about the land, soil, *etc.*; and smart health care systems, which provide the health status of individuals [2]. Since it can be

[*] **Corresponding author K.K. Sowjanya:** Dayananda Sagar University, Bangalore; E-mail: ksowjanya-cse@dsu.edu.in

Rashmi Agrawal and Neha Gupta (Eds.)

used in day-to-day activities, the usage of these IoT devices is enormous in various fields like health care, industries, agriculture, cities, *etc.* The usage statistics of IoT devices in various fields in 2020 are represented in Fig. (**1**) as follows:

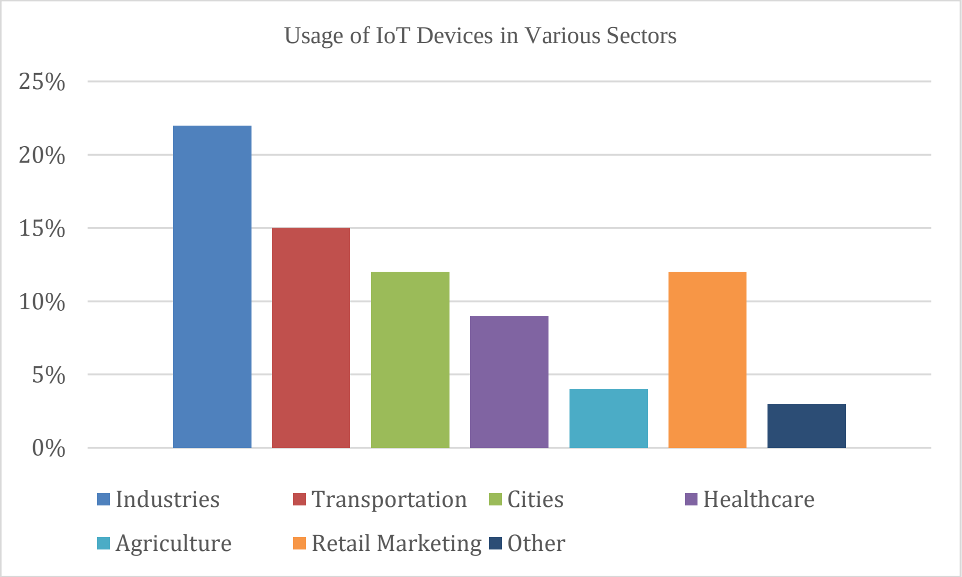

Fig. (1). Usage of IoT Devices in Various Sectors [3].

IOT ARCHITECTURE

Fig. (**2**) depicts the IoT's core three-layer architectural structure in terms of the devices and technology that each layer encompasses. Each layer in the IoT is characterized by the functions it performs and the devices it employs. Many experts believe that the IoT is primarily based on three layers: perception, network, and application [4].

Perception Layer: It is the architecture's physical layer. This is where the sensors and connected devices come together when they collect different amounts of information according to the project requirements. The edge devices, sensors, and actuators which interact with their environments can be used.

Network Layer: All of the data gathered by these devices must be transferred and processed. This is the role of the network layer. These devices are linked to other smart things, servers, and network devices. The transmission of all the data is also handled. Cloud computing platforms, Internet gateways, switching and routing devices, and other devices at this layer use cutting-edge technologies, including Wi-Fi, LTE, Bluetooth, 3G, and Zigbee.

Application Layer: The user interacts with the application layer. It's responsible for providing the user with application-specific services. This might be a smart home application where users tap a button in the app to switch on a coffee machine, for example. The data's validity, integrity, and confidentiality are all guaranteed by the application layer. The goal of IoT, or the establishment of a smart environment, is accomplished at this layer.

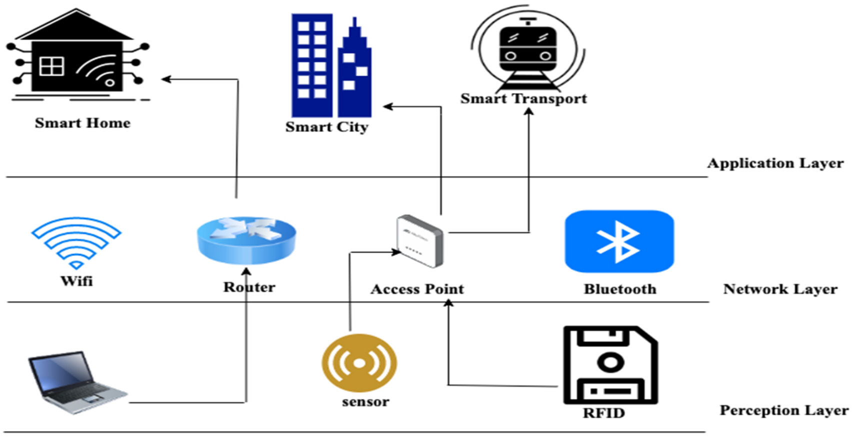

Fig. (2). Three-Layer IoT Architecture [5].

IOT FITBIT INTRODUCTION

James Park and Eric Friedman launched Fitbit Incorporated in 2007 as Healthy Metrics Research Incorporated. The initial goal of the company was to incorporate accelerometers into wearable technology. Accelerometers are small sensors that measure the forces of acceleration. The Fitbit Tracker, the company's first product, was released to the public in 2009. The first Fitbit was a wristband that was attached to the wearer's clothing. The little device could count and track the number of steps taken, and it was followed by a slew of other Fitbit gadgets with a variety of features. An accelerometer is used in Fitbit devices to track your movements. Fitbit counts your steps and monitors the distance you've gone, calories burnt, and sleep quality using the accelerometer, which converts movement data into digital measures. Fitness tapes include a touchscreen, smartphone notifications, activity, and medical monitoring, automatic exercise detection, and water resistance to swimming. It has a built-in heart rate monitor and sleep tracking. Calls, texts, and calendar reminders are also available for notifications on the band. During the day, the Fitbit Tracker could be fastened to the user's clothing. It also came with a wristband so you could wear it at night. The device was linked to a website where users could log their workouts, eat their meals, and keep track of their weight. It also included a charging station that allowed customers to wirelessly upload data from their Fitbits.

CHAPTER 7

Blockchain Based Access Control Systems

R. Agrawal[1,*] and **N. Gupta**[1]

[1] *Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India*

Abstract: While accessing data through the Internet of Things (IoT), privacy and safety are the most important features. IoT developers have a challenging job of securing and protecting the data of the users during the development process due to the complicated nature of decentralisation and heterogeneity of the environment present in IoT. There are several access control models for the IoT available in the literature which rely on centralized architecture and raises security concerns because IoT devices can spontaneously and dynamically interact with one another. The need for secure and distributed access control architecture to overcome the single point of failure problem of a centralized entity becomes a big challenge when coupled with scalability and lightweight features. It is possible to achieve this through the use of Blockchain technology, which has recently been used to provide access control services. IoT device management would be used to manage distribution, heterogeneity, scalability, the ability to tolerate failure, security and privacy aspects of IoT devices at scale in the near future as it is useful.

Keywords: Blockchain, Access control system, Policy creation transaction, Distributed access management, Internet of things.

INTRODUCTION

There seems to be a reliance on the presence of a trusted authority in the current digital economy. To conduct any online transaction, we need to trust that the information we receive is accurate. Whether that be an email service provider informing us of delivery or a certification authority telling us to trust a particular digital certificate; on the other hand, a social network, for instance Facebook, might tell us our posts about life are only shared with our friends, or a bank might tell us we can put our trust in our dear ones in another country. We live in a world that is precarious, where we have to rely on a third-party institution to keep us safe and to keep our individual information private. Third parties, as always, are susceptible to hacking, manipulation, or compromise. Blockchain technology offers a solution to these problems. With distributed consensus enabled by this

[*] **Corresponding author R. Agrawal:** Manav Rachna International Institute of Research & Studies, Faridabad, Haryana, India; E-mail: rashmi.fca@mriu.edu.in

Rashmi Agrawal and Neha Gupta (Eds.)

technology, it is possible to verify any online transaction involving digital assets at any time, allowing the world of digital to undergo revolutionary change. Digital assets and party identities are protected without compromising privacy. Blockchain technology is distinguished by its distributed consensus as well as its anonymity. Regulation issues and technical challenges are outweighed by the benefits of Blockchain technology.

Blockchain technology has proven to be a highly transparent and incorruptible method of storing data. Decentralized technology ensures encryption and security end-to-end, making it ideal for networks with lots of users. Blockchain's decentralized nature eliminates the possibility of human error and offers protection against hacker attacks altogether due to its distributed nature. In the context of Access Control, especially Access Control as a Service, all of the above is of paramount importance.

Cryptocurrencies and financial transactions were the first blockchain applications. There is a wide range of applications for smart contracts, such as healthcare, internet of things, supply chains and more. Study [1], a review of many research studies on blockchain and smart contracts, shows that many of the applications presented were aimed at providing an efficient and secure way to control access.

An Access Control System is used to control access to data and services that are perceived as critical or valuable by the public. Furthermore, it is also used to manage computing systems, storage space, and other coprocessors. Access control policies are used in general to express the rights of subjects to access resources. These policies are evaluated based on the context of the request at the time. ABAC (Attribute-Based Access Control) [2] is a form of access control that consists of a set of conditions that describe the inherent characteristics of subject areas, resources, environments, *etc.,* involved in the access request. As examples of subject attributes, one can find his ID, the company's ID, his title within that organization, the names of the projects he is working on, the number of resources he is currently using, and so on.

It may be necessary to transfer the access right between subjects for a variety of reasons in some cases due to certain circumstances. An individual who owns an access right could, for instance, sell it to someone else. The same holds true for an example of an employee of a company who is supposed to perform a particular procedure on a Virtual Machine, yet chooses rather delegate the responsibility of the task to another employee who also needs to access the Virtual Machine.

BACKGROUND

A blockchain is a digital ledger of data that can be accessed by anyone at any time. Blockchains are decentralized databases that are secure, easy to use, and can be accessed by anyone. This system is based on trustless principles, which means that users accept the data and analyze the data, whether it is secure or not, without any third-party intervention. Initially, it was planned to provide secure cryptocurrencies, such as Bitcoins, but nowadays, researchers are exploring the possibility of applying the technology to a wide range of fields [3]. As part of the method, tokens are exchanged in the form of transactions on the blockchain in exchange for tokens. A blockchain is an example of a peer-to-peer network consisting of several nodes that uses a cryptographic protocol. By verifying the transactions and passing between these nodes, these nodes handle the communication between them. Blockchain has a lot of interesting features that make it easy to use [4]. Basically, it is a distributed ledger that is only appended to. The data, once inserted into a database, cannot be changed once they have been added, nor can they be deleted after they have been added. On the blockchain, anyone can be added to the network, so they will be able to see all the transactions that are by nature public, as blockchain transactions are public by nature.

With the help of the blockchain, bitcoin, like many other cryptocurrencies, stores value exchanges referred to as transactions on the public ledger [5]. Every single block in this ledger is a collection of non-conflicting transactions that were made in that block. In order to create the link between blocks, the hash of the header of the previous block is stored in the header of the next block of the chain. The root of a Merkle tree derived from the block transaction hashes is included in the block header of each block as a function of its block header (and hence it is hash). This is done to make the block headers dependent on all transactions contained in that block. The decision of which block to add to the ledger at each step is made by a distributed consensus algorithm known as the 'Nakamoto consensus', which is based on the HashCash Proof-of-Work [6] system.

A simple way to look at the Bitcoin blockchain from a data point of view is to see it as a list of transactions. Users exchange funds using their wallet addresses, which serve as the address of their wallet. A public key that derives from an ECDSA key pair [7] is derived as a two-way hash (first applying SHA-256 and then applying Ripemd-160 as the second step) to establish an address.

In the case of Bitcoin, the address (and therefore the public key) is used by the users to send and receive payments, while the private key is used to provide proof of ownership (through digital signatures). Since creating new ECDSA key pairs is

CHAPTER 8

Multi-chain Deployment over Smart Contracts to Enhance Security

N. Gupta[1,*] and **R. Agrawal**[1]

[1] *Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India*

Abstract: A blockchain is a data structure in which each block is linked to the next in a time-stamped chronological manner. Each block is cryptographically linked to the others. This is a global distributed ledger that contains an immutable public record of financial transactions. Every new record will be reviewed across the distributed network before being saved in a block. All information is verifiable and auditable once it is deposited on the ledger, but it cannot be edited. It will be an underestimation to say that Blockchain Technology is one of the most inventions of this 21st century. More people are considering that the decentralization and translucence that comes along with blockchain technology have the prospective to jiggle multiple industries to its very staple. This article reconnoiters different blockchain applications and their deployment approaches. In other facets, Multichain is a platform for the creation and distribution of private blockchains, either within or between organizations. Likewise, there are many more blockchain applications than just cryptocurrency, and they can unsettle way more sectors than just the finance sector. We intentionally avoided showing the Blockchain's impact on the banking sector to keep the list as non-fintech as possible. Smart contracts are well customary as the greatest enabling technology for blockchains. With them, a blockchain ecosystem becomes self-governing, open, consent, and credible. It is through a compilation of smart contracts that blockchains can operate without human intervention.

The smart contracts are established to deploy at the predefined blockchain nodes. They can be entreated by the call-backs either from the blockchain system, the other smart contracts, or the participants' information systems.

Usually, blockchain operations and application-related rules can be predetermined as smart contracts. The use cases and their real-world functions differ, but the benefits derived from using the technology remain unchanged: immutability, transparency, redundancy, and security.

Keywords: Multi chain, Block chain, Real world applications, Decentralization, Smart contracts.

[*] **Corresponding author N. Gupta:** Manav Rachna International Institute of Research & Studies, Faridabad, Haryana, India; E-mail: neha.fca@mriu.edu.in

Rashmi Agrawal and Neha Gupta (Eds.)

INTRODUCTION

The Blockchain is a series of blocks, each of which holds valuable data that is not supervised by a central authority. It is unchangeable and cryptographically secure. Linked Lists and Pointers are two significant data structures used in a blockchain. The Blockchain is redefining ways of handling trustworthy transactions. The internet is incredibly vulnerable, and Blockchain [1] has been released as a result of this. Blockchain defines the confidence liability lines as one challenge for AI and IoT. The majority of IoT devices communicate with one another on public networks, and it is superfluous to discuss how vulnerable public networks are. Blockchain [2] overcomes this challenge by allowing users to create linear and long-lasting indexed records. They can also make the business process go more smoothly by offering a payment mechanism and a communication channel. Any kind of hacking and tampering with the data, like captivating control of devices and records, is excruciating by the way blocks are stored and guarded in an unambiguous database in the Blockchain outline. Every IoT device is a point of vulnerability, and the hazards are still higher as even AI is intricate in making choices for users. Hence, Blockchain can provide a safe, scalable, and certifiable platform with superlative security implementations [3].

BLOCKCHAIN AND SMART CONTRACTS

Implementation Techniques for Blockchains

To develop a realistic and effective blockchain application environment, a number of fundamental concerns must be addressed [4]. The four levels of a unique blockchain ecosystem are smart contracts, Blockchain, services, and user interfaces. Enterprise network models, participants, ecosystem design, admission policies, nodes, polling systems, incentive mechanisms, smart contracts, and clients are all examples of blockchain implementation strategies. Furthermore, to solve the problematic issues of blockchain applications, data collecting and data processing methods are required.

The majority of current projects are struggling with the blockchain network concept [5]. Blockchain technologies are still changing, and no widely acknowledged technological pattern exists. Due to their inefficiency and high-performance costs, specific Bitcoin-based projects have not been recognised. Self-designed hybrid networks or alternative network architectures are being used in an increasing number of applications.

A typical blockchain ecosystem includes a blockchain infrastructure, participants' information systems with programming edges to the Blockchain, and a set of smart contracts for operation. All data and communications are stored in a decentralised and self-regulating data infrastructure provided by the blockchain system.

Participants should be identified based on their function and the blockchain network. The polling technique and operation objectives determine the number of nodes and evolution policies. The network model is used to establish the admission policies and required information in the consortium blockchain paradigm. To build the Blockchain and establish an effective consensus process, a realistic and efficient incentive mechanism should be developed.

Smart contracts are often regarded as the most advanced blockchain-supporting technology. A blockchain ecosystem that includes smart contracts improves autonomy, openness, consent, and credibility. Blockchains can work without the need for human intervention thanks to a collection of smart contracts. Smart contracts are created with the intention of being implemented at predetermined blockchain nodes. Call-backs from the blockchain system, other smart contracts, or the parties' information systems can all be used to activate them. Smart contracts may usually be used to programme both blockchain operations and application-related rules.

Blockchain Clients for Participants

There are three different types of blockchain clients, each of which interacts with the blockchain ecosystem *via* application programming interfaces. The first sort of client is created in the information systems of the participants; this includes both management information systems and embedded systems. Smart contracts, or those given by the Blockchain operating systems, such as blockchain browsers, are the second type of client. The Blockchain's third form of the client is public facilities, which provide a public user interface for both participants and potential participants.

To support blockchain-based enterprises, data collection approaches are precarious. The data in a blockchain is intended to be private and self-regulated by the members, which poses a number of common data collection difficulties, including data insufficiency, data scarcity, and data redundancy. For missing data attributes and irrelevant or redundant data, well-defined compensation methods must be developed. Simultaneously, weighing and cross-checking algorithms should be developed to take advantage of the assimilated participatory data from both inside and outside the Blockchain, on and off the Blockchain, which could be implemented as smart contracts to consolidate the data. When administering the data, there are a few additional concerns to consider. For example, to learn how to make use of data from previous blockchain ecosystems, the ecosystem is built to

CHAPTER 9

Blockchain for Decentralized Services: On Improving Security and Performance of Distributed IPFS-based Web Applications

V. Le[1], R. Moazeni[1], M. Moh[1], R. Agrawal[2,*] and **N. Gupta[2]**

[1] *San Jose State University, San Jose, CA 95192-0249, USA*

[2] *Manav Rachna International Institute of Research and Studies, Faridabad, India*

Abstract: While cloud computing is gaining widespread adoption these days, some challenges are emerging around the security, performance, and reliability of centralized cloud resources. Decentralized services are introduced as an effective way to overcome the limitations of cloud services. Blockchain technology, with its associated decentralization, is used to develop decentralized application platforms. The Interplanetary File System (IPFS) is built on top of a distributed system consisting of a group of nodes that shares the data and takes advantage of blockchain to permanently store the data. The IPFS is very useful in transferring remote data. This work focuses on applying blockchain technology to the IPFS to improve its security and performance. It illustrates different types of blockchain and their advantages and challenges; it also describes the proposed design and its detailed implementation. For performance evaluation, we show the performance gains, analyze security enhancements, and discuss the tradeoffs between security and performance. The presented work is significant towards more secure, efficient web applications utilizing emerging blockchain technologies.

Keywords: Blockchain technology, Distributed system, Decentralized service, Interplanetary file system (IPFS).

INTRODUCTION

Blockchain is a progressive innovation set to change the eventual fate of processing and disturb a few businesses with additional inventive arrangements. It is open, changeless and appropriate for all means and purposes relevant to a variety of scenarios. The innovation increased enormous intrigue from the ascent of digital forms of money; however, it sees applications in numerous different divisions other than funds. Businesses and government organizations are using

[*] **Corresponding author R. Agrawal:** Manav Rachna International Institute of Research and Studies, Faridabad, India; E-mail: rashmi.fca@mriu.edu.in

Rashmi Agrawal and Neha Gupta (Eds.)

centralized cloud resources increasingly these days. Amazon AWS, Google Cloud, and other popular services provide a high level of security and reliability [1]. Using centralized cloud resources, however, has some limitations since the centralized cloud can be a single point of failure, as many examples in the past have shown. Take, for example, a careless mistake committed by a cloud operator that can cause the cloud, and all the companies and organizations relying on the cloud resource, essentially half of a country, to shut down for up to an entire day. Similarly, a power outage, a data loss, or a network attack on these services can potentially disrupt operations, causing huge damage to user data and business activities [2]. A survey was conducted by Right Scale in 2018; it asked 997 technical professionals about the challenges of adopting cloud technology. The survey showed some interesting findings. Security was the top concern mentioned by 77% of them, and 55% of them faced performance challenges while using cloud technology [3].

In the paper, Hassanzadeh-Nazarabadi *et al.* (2019), the author used the distributed hash table concept to design a blockchain architecture called LightChain. LightChain is a permissionless blockchain where any node can join the network. Any new transaction or block addition to this blockchain will be recorded in the distributed hash table of a peer in an on-demand manner, so each peer does not have to store the entire blockchain locally [4]. Although distributed hash tables provide efficient data lookup, they may take a noticeable amount of time when a lot of table searches are required to retrieve data.

The security and performance challenges of distributed systems are discussed in this chapter. The drawbacks of centralized cloud resources can be mitigated by blockchain-based solutions. As blockchains are stored on ledgers that are shared between all participating nodes on a network, they have the right characteristics and functionalities to handle these kinds of computations decentrally and by multiple parties. In addition, any transaction that takes place on the blockchain requires the consensus of all the nodes, so it is also very secure. Blockchain technologies, therefore, have been recommended to be used for achieving distributed, fault-tolerant consensus and for building efficient public-key-based secure infrastructures. It is important that there is no single entity that controls the blockchain, so it does not have the single point of failure issue as in other regular cloud storages [4].

A new file system called the interplanetary file system (IPFS) is designed to process large files decentralized and effectively [5]. The IPFS network operates on a peer-to-peer basis, with each peer providing its own storage. It helps prevent data losses since the same data is available on multiple peer nodes [6]. Based on the above reasons, IPFS combined with blockchain technology can serve as a great solution to address the security and performance concerns of cloud technology.

An approach to securing distributed web apps using blockchain and smart contracts is described in this article, which includes smart contracts to control access to IPFS [7]. The detailed implementation is depicted, including encryption/decryption schemes, smart contracts, remote application migration, and memory cache for key values. Performance and security analyses are presented, with a discussion of tradeoffs between the two.

This chapter is a substantial extension of earlier work. The rest of the chapter is organized as follows. Section II goes over preliminary background information and related work about blockchain technology, smart contracts, IPFS, distributed hash table, and memory cache [8]. Section III demonstrates the high-level architectural design of the web application as well as how each component is designed. Section IV talks about the implementation of each improvement method in our application. In Section V, we detail our experiments and analyze the performance and security aspects of our application. Finally, Section VI presents the conclusion and future work.

BACKGROUND AND RELATED WORK

Background of Blockchain Technology

Blockchain is a decentralized, public ledger that tracks online transactions. A decentralized blockchain ledger maintains a shared record of all the transactions distributed over a large user network. This is a completely decentralized network, which does not require any intermediary mechanism for exchanging services. A blockchain is a series of data blocks, in which a small patch of user-made transactions is stored in each row. Both these data blocks are clustered together electronically, using a top-tier level of cryptography [9]. Both of the blocks together then form a permanent and malicious public record of each and every transaction that occurs on the network. The user is connected to a blockchain in such a way that his / her data is made accessible without revealing their identity to any other user in that blockchain. Blockchain offers users complete transparency to make things simpler [10]. Through encrypting and validating, Blockchain guarantees the confidentiality, authenticity and privacy of transactions. By adding a new block to a blockchain, a cryptographic hash generated from the previous block’s content is used to link it to the preceding block. It means the chain never breaks, and each block is registered forever [11]. Consequently, this is deliberately difficult to alter past blockchain transactions, as all subsequent blocks must be modified first. Blockchain databases are made up of many nodes, and decentralized. Administration includes the node: all nodes review recent

SUBJECT INDEX

Rashmi Agrawal and Neha Gupta (Eds.)

R. Agrawal

Dr Rashmi Agrawal is PhD and UGC-NET qualified with 22 years of experience in teaching and research, working as Professor in Department of Computer Applications, Manav Rachna International Institute of Research and Studies, Faridabad, India. She is life member of Computer Society of India and senior member of IEEE, She is book series editor of many series with reputed publishers like Wiley and CRC press. She has authored/ co-authored 80+ research papers in peer reviewed national/international journals and conferences which are SCI/SCIE/ESCI/SCOPUS indexed. She has also edited/authored books with national/international publishers (Springer, Elsevier, IGI Global, Apple Academic Press, and CRC Press) and contributed chapters in books.

N. Gupta

Dr. Neha Gupta has done her PhD from Manav Rachna International University and has total of 17+ year of experience in teaching and research. She is a Life Member of ACM CSTA, Tech Republic and Professional Member of IEEE. She has authored and coauthored 80 research papers in SCI/SCOPUS/Peer Reviewed Journals (Scopus indexed) and IEEE/IET Conference proceedings in areas of Web Content Mining, Mobile Computing, and Cloud Computing. She has published books with publishers like Springer, Taylor & Francis, IGI Global & Pacific Book International and has also authored book chapters with Elsevier, Springer, CRC Press and IGI global USA. She is a technical programme committee (TPC) member in various conferences across globe.