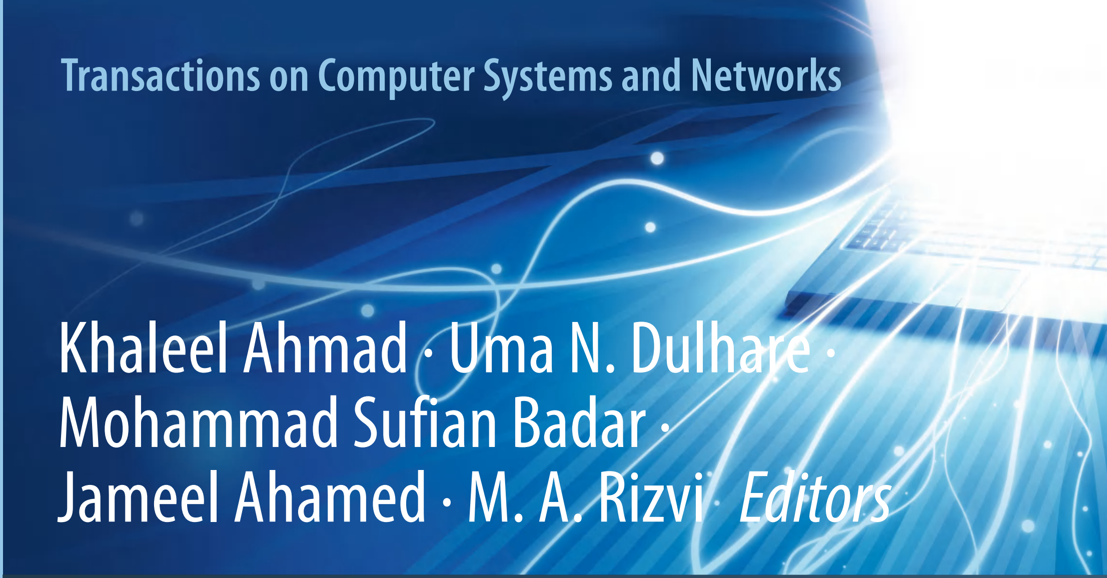
Transactions on Computer Systems and Networks



Khaleel Ahmad · Uma N. Dulhare ·
Mohammad Sufian Badar ·
Jameel Ahamed · M. A. Rizvi *Editors*

Fostering Machine Learning and IoT for Blockchain Technology

Smart Cities Applications, Volume 2

Springer

Transactions on Computer Systems and Networks

Series Editor

Amlan Chakrabarti, Director and Professor, A. K. Choudhury School of Information Technology, Kolkata, India

Editorial Board

Jürgen Becker, Institute for Information Processing–ITIV, Karlsruhe Institute of Technology—KIT, Karlsruhe, Germany

Yu-Chen Hu, Department of Computer Science and Information Management, Providence University, Taichung City, Taiwan

Anupam Chattopadhyay, School of Computer Science and Engineering, Nanyang Technological University, Singapore, Singapore

Gaurav Tribedi, Department of Electronics and Electrical Engineering, Indian Institute of Technology Guwahati, Guwahati, India

Sriparna Saha, Department of Computer Science and Engineering, Indian Institute of Technology Patna, Patna, India

Saptarsi Goswami, A. K. Choudhury School of Information Technology, Kolkata, India

Transactions on Computer Systems and Networks is a unique series that aims to capture advances in evolution of computer hardware and software systems and progress in computer networks. Computing Systems in present world span from miniature IoT nodes and embedded computing systems to large-scale cloud infrastructures, which necessitates developing systems architecture, storage infrastructure and process management to work at various scales. Present day networking technologies provide pervasive global coverage on a scale and enable multitude of transformative technologies. The new landscape of computing comprises of self-aware autonomous systems, which are built upon a software-hardware collaborative framework. These systems are designed to execute critical and non-critical tasks involving a variety of processing resources like multi-core CPUs, reconfigurable hardware, GPUs and TPUs which are managed through virtualisation, real-time process management and fault-tolerance. While AI, Machine Learning and Deep Learning tasks are predominantly increasing in the application space the computing system research aim towards efficient means of data processing, memory management, real-time task scheduling, scalable, secured and energy aware computing. The paradigm of computer networks also extends it support to this evolving application scenario through various advanced protocols, architectures and services. This series aims to present leading works on advances in theory, design, behaviour and applications in computing systems and networks. The Series accepts research monographs, introductory and advanced textbooks, professional books, reference works, and select conference proceedings.

Khaleel Ahmad · Uma N. Dulhare · Mohammad Sufian Badar · Jameel Ahamed · M. A. Rizvi
Editors

Fostering Machine Learning and IoT for Blockchain Technology

Smart Cities Applications, Volume 2

Springer

Editors
Khaleel Ahmad
Maulana Azad National Urdu University
Hyderabad, Telangana, India

Mohammad Sufian Badar
Department of Bioengineering
University of California, Riverside
Riverside, CA, USA

M. A. Rizvi
National Institute of Technical Teachers
Shamla Hills
Bhopal, Madhya Pradesh, India

Uma N. Dulhare
Sagar Society, Srinagar Colony
Plot 65, Near Karnataka Bank
Hyderabad, Telangana, India

Jameel Ahamed
Maulana Azad National Urdu University
Hyderabad, Telangana, India

ISSN 2730-7484 ISSN 2730-7492 (electronic)
Transactions on Computer Systems and Networks
ISBN 978-981-96-4073-7 ISBN 978-981-96-4074-4 (eBook)
https://doi.org/10.1007/978-981-96-4074-4

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2025

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

If disposing of this product, please recycle the paper.

This book is dedicated to those who volunteered to save the lives of thousands of people. In the holy Quran, Surah 5, Ayat 32, it is mentioned that saving one person's life is equivalent to saving all of humanity and the Prophet Muhammad (pbuh) said, "The best of people are those that bring most benefit to the rest of mankind", which compelled me to author a book that can save the lives of many people worldwide, by providing them information to make informed decisions. I am grateful to my parents, (Amman, Marhooma Nurunnisa, Abba Marhoom Mohd. Badre Alam), mother in laws, Fakhrun Nisa Kamal, wife, Rana Kamal Sufian, sister, Shahnaz Badar, daughters; Sarah Sufian Badar and Aisha Sufian Badar, brothers, nieces and nephews. Their support, encouragement, guidance, and constant love have sustained and encouraged me.

Preface

In the modern era, integrating machine learning, Internet of Things (IoT), and blockchain technology has the transformative potential to shape smart urban development. “Fostering Machine Learning and IoT for Blockchain Technology Smart Cities Applications” has taken the initiative, so that the readers will be able to understand how these cutting-edge technologies can collaborate to enhance smart city applications.

This book is written to bring awareness to the methods used for blockchain in the academic and professional community. Volume I book is organized into 13 chapters. This book will discuss blockchain with IoT and Big Data. It will also explain how this technology can be used to improve Healthcare, Police Management, and Cybersecurity.

Volume I book is organized into 13 chapters. It covers the concepts of blockchain like cryptography, then it gives an introduction to blockchain technology, covering topics, viz. consensus mechanisms, architecture, and enterprise solutions for modern business applications, such as Hyperledger Fabric. It also emphasizes private and consortium blockchains, along with practical applications, such as lightweight encrypted police management system for enhancing public safety and data management. This is done on a blockchain-based serverless platform using the Blowfish algorithm to emphasize the importance of efficient data handling in smart city solutions. It covers Volume II book that is organized into 10 chapters. It encompasses a diverse range of innovative applications with a fusion of blockchain technology, IoT, and machine learning.

The application of Blockchain in Supply Chain Management delves into how blockchain enhances traceability, transparency, and efficiency in supply chains promoting trust among the stakeholders. “Banking with Blockchain Technology” explores how blockchain can enable faster transactions, reduced costs, and enhanced security. Blockchain with cyber-physical systems in smart cities ensures the integrity and security of the interconnected infrastructure. The chapter “Towards Secure Healthcare IoT—Opportunities and Challenges of Blockchain” addresses challenges in advances in patient data. Blockchain and IoT have been used to enhance the efficiency and reliability of Uzbekistan’s railway systems in a digital economy.

"Integrating Machine Learning" and the chapter "Blockchain with UAV Routing and Navigation—Challenges and Potential Solutions" focus on optimizing drone navigation systems. "Smart Irrigation and Climate Resilience: Leveraging IoT and Blockchain for Sustainable Agriculture" explores how blockchain and IoT technologies can improve agricultural practices and water management, contributing to climate resilience and sustainability. "Blockchain Application in Smart Water and Waste Water Management" explains how blockchain can optimize smart water management systems, ensuring efficient and sustainable usage of water resources.

Through this book, our aim is to showcase the transformative potential of integrating machine learning, IoT, and blockchain technologies in smart city applications which will be secure, efficient, and sustainable. It will also focus on contemporary topics for research and development.

Hyderabad, India	Khaleel Ahmad
Hyderabad, India	Uma N. Dulhare
Riverside, USA	Mohammad Sufian Badar
Hyderabad, India	Jameel Ahamed
Bhopal, India	M. A. Rizvi

Acknowledgment

First and foremost, I would like to praise and thank Allah SWT, the almighty, who has granted me countless blessings, knowledge, and opportunities so that I can edit my this book.

I am extremely grateful to my parents (the late Mohd. Badre Alam and Nurunnisa) for their love, prayers, caring, and sacrifices in educating and preparing me for my future. Most importantly, I thank my wife, Rana Kamal, and daughters, Sarah Sufian Badar and Aisha Sufian Badar, for their patience, assistance, support, and faith in me. Rana's tolerance of my occasional lows is a testament in and of itself to her unyielding devotion and love.

I am also thankful to my mother-in-law, Fakhrun Nisa Kamal and her brother Janab Shamsud Tauhid Saheb, Dr. Azfar Kamal, Dr. Farheen Asaf Kamal, Feraz Kamal, Farha Kamal, Shaheen Kamal, Mohd Salahuddin and their children, Yusuf, Ibrahim, Abdullah, Maryam, and Ammar.

I will forever be thankful to my sister (Shahnaz Badar), my brothers (M. Rizwan Badar, M. Hassan Badar (Marhoom), Dr. M. Affan Badar, and Dr. M. Rehan Badar), my sisters-in-law (Sayyada Shaheen, Mahtab, Dr. Sadia Saba, and Ishrat Raza), brother-in-law (late Professor Md. Zaki Ahmed), niece: Dr. Aafia Tasneem, Dr. Labeebah Nesa and her spouse, Dr. Yaqoot Taban Khan, Aalia Tasneem, and her spouse, Mansoor Alam, Sidrah, Isra, Samiyah, Samra, nephew: Aamir Nehal and his wife, Shazia Tamkin and their children (Aayaan Aamir, Eshaan Aamir, Anabia Aamir), Aadil Jamal and his wife Dr. Samreen Rahman, Aasim Kamal, his wife Mahwish Khan and his daughter Fatima, Aatif Belal and his wife, Areej Masood, Mobashshir, Modabbir and his wife Dr. Zainab Imtyaz, Modassir, Maaz, Mauviz, Ibrahim, Ismail, and my only Mamani, Naushaba Marhooma for their support and valuable prayers. It would be incomplete if I didn't mention my cousin, Brother Saud Aslam 'Arshi', Brother Saeeduzzafar/Rashiduzzafar/Sultan Zafar/Tanweer Alam/Tauseef Alam/Tauqeer Alam/Tafseer Alam (Sajjad), sister Tahira, Zahera, Nazli, Ruby, Shazli, all family members of "Ahle Nawaab Jaan", all members of our model village, Nazra.

I want to mention my beloved Chachi Tahira Khatoon Saheba, Mokhlis phoophi, Soghra Jamal Saheba, Mokhlis phoophi Ishrat Jamal Saheba, and Mokhlis phoophi Yasmeen Perween (Gauhar) Saheba. It is unfair if I didn't mention my youngest chacha, Iqbal Ahmed, sister Ghazala Yasmin (Guria), brother Salman Akhter (Retired Govt Employee), brother Iqbal Akhter, Kaleem Ahmed (Narainpur), Rafeul Hoda, Tanweer Ahson, and brother Maswood Akhter ("Master saheb"). Thank you brother Ali Murshid Zeya Arshi who has written these two lines only for this book,

بیش قیمت ہے انسان کی زندگی
تم بچائو اسے ہے یہی بندگی

As a member of Ahle Nawaab Jaan, we have been suffering from internal disputes, which have gone to such a level that we are filing false cases against each other. Both of my chachas are very Mokhlis to each of us and have contributed socially, financially, and academically. As we know Shaitan is our open enemy, and Shaitan has trapped all of us. Amongst our neighboring areas and extended family, they still don't believe that cases have been filed against each other. I came to know that both Chachas are very much NAADIM and continuously doing Dua, but Shaitan is not giving them any opportunity so they can withdraw the cases. Recently, I spoke to a family member and he told me that he avoids going to the Mosque due to this situation and he doesn't sit after Fajr prayer because of this situation.

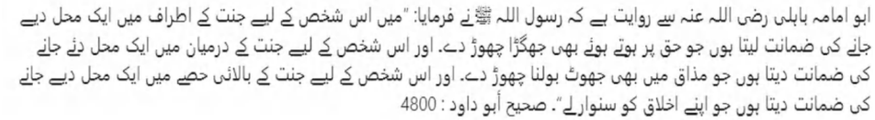
It is good practice to follow the Sunnah, footsteps of our fathers and forefathers, though you have to suffer sometimes financially. Since this was the common RAASTA at the time of our all beloved Dadas, it is best that we don't disturb it out of respect for our fathers and forefathers and common people of my beloved villagers.

It is my humble request that we should lead by example by leaving all the negative things that happened during the last two years in the past. We need your guidance, support, and suggestions at this moment and lead our Khandan.

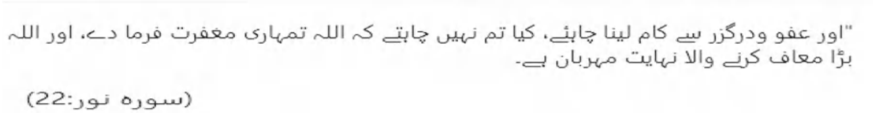
O'Allah, please forgive us and show us the right path which leads to paradise.

O'Allah my beloved Chachi is not well, please provide her complete SHIFA because she is the one who motivated and encouraged my chacha for this noble act. The names of my Chachas are Janab Omar Khalid Saheb and Janab Mahmood Alam Saheb. I would like to THANK my Chacha Janab Omar Tarique Saheb, Chacha Janab Omar Rashid, Phoopha Ahmed Karimi, Zakia Phoophi, and Razia Phoophi who asked both of my Chachas for this charity with the sole purpose of maintaining the relationships among the members of Ahle Nawaab Jaan and Ahle Nazra.

The reward for this noble act is,

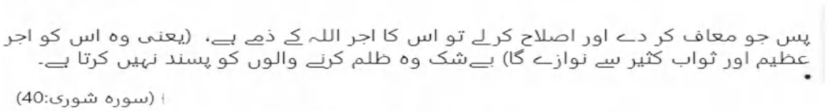


ابو امامہ باہلی رضی اللہ عنہ سے روایت ہے کہ رسول اللہ ﷺ نے فرمایا: "میں اس شخص کے لیے جنت کے اطراف میں ایک محل دیے
جانے کی ضمانت لیتا ہوں جو حق پر ہوتے ہوئے بھی جھگڑا چھوڑ دے. اور اس شخص کے لیے جنت کے درمیان میں ایک محل دئے جانے
کی ضمانت دیتا ہوں جو مذاق میں بھی جھوٹ بولنا چھوڑ دے. اور اس شخص کے لیے جنت کے بالائی حصے میں ایک محل دیے جانے
کی ضمانت دیتا ہوں جو اپنے اخلاق کو سنوار لے". صحيح أبو داود : 4800



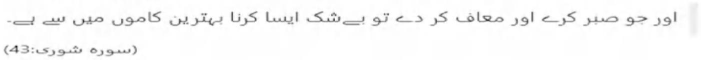
"اور عفو ودرگزر سے کام لینا چاہئے، کیا تم نہیں چاہتے کہ اللہ تمہاری مغفرت فرما دے، اور اللہ
بڑا معاف کرنے والا نہایت مہربان ہے۔

(سوره نور:22)



پس جو معاف کر دے اور اصلاح کرلے تو اس کا اجر اللہ کے ذمے ہے، (یعنی وہ اس کو اجر
عظیم اور ثواب کثیر سے نوازے گا) بےشک وہ ظلم کرنے والوں کو پسند نہیں کرتا ہے۔

(سوره شوری:40)



اور جو صبر کرے اور معاف کر دے تو بےشک ایسا کرنا بہترین کاموں میں سے ہے۔

(سوره شوری:43)

Contents

Editors and Contributors

About the Editors

Dr. Khaleel Ahmad is currently an Assistant Professor in the Department of Computer Science and Information Technology at Maulana Azad National Urdu University, Hyderabad. He has more than nine years of teaching and research experience. He worked as a Visiting SERB International Research Fellow in the Department of Computer Science, University of Pisa, Italy, under the SERB International Research Experience (SIRE) Fellowship Programme funded by the Science and Engineering Research Board (SERB), Government of India for six months. He visited the National Defence University of Malaysia, Malaysia as a Visiting Faculty from 26 December 2018 to 6 January 2019. He completed one Research Project of 01.05 Lakh. He received a UGC-MANUU National Travel Grant in 2014. He has received the best paper award at two conferences in Malaysia and India. He coordinated two Faculty Development Programmes sponsored by DRDO and NITTTR, Bhopal. He has supervised one Ph.D. student, seven M.Tech. students, and several B.Tech. students, along with many MCA research projects. His research areas are Blockchain Technology, Cyber Security, Cryptography, and Opportunistic Networks. He has filed two patents from Malaysia in collaboration with the National Defence University of Malaysia. He has published more than 50 papers in refereed Journals and conferences (viz. Nature, Elsevier, ACM, IEEE, and Springer) and 20 book chapters (Springer, Taylor & Francis, Wiley, IGI Global). He has edited four books published by Springer, Taylor & Francis, and Wiley. He has delivered lectures in India and abroad and chaired several sessions at National and International conferences. He is a life member of various international/national research societies viz. ISTE, CRSI, ISCA, IACSIT (Singapore), IAENG (Hong Kong), ISOC (USA). In addition, he is associated with many international research organizations as an editorial board member and reviewer.

Prof. Uma N. Dulhare is currently working as a Professor and head of the Department of Computer Science and Artificial Intelligence, MuffaKham Jah College of Engineering, Hyderabad, India. She has more than 20 years of teaching experience.

She received her Ph.D. from Osmania University, Hyderabad. Her research interests include Data Mining, Big Data Analytics and Machine Learning, IoT, Cloud computing, and Biomedical Image Processing. She has published over 30 research papers in reputed National and International Journals and book chapters. Also, she edited three books. She is a Member of the Computer Science Teachers Association (CSTA), USA, IEEE (SMC), ACM, Senior Member of the International Association of Engineers (IAENG), Senior Member of Universal Association of Computer and Electronics Engineers (UACEE) Life Member of ISTE.

Dr. Mohammad Sufian Badar Ph.D. has served as a Senior Teaching Faculty in the Department of Bioengineering at the University of California, Riverside, CA, USA. He served as an Analytics Architect in CenturyLink for over a year in Denver, CO, USA. Currently, he has been serving as a senior faculty (temporary) in the Department of Computer Engineering at Jamia Hamdard, New Delhi, India. He possesses an excellent academic record with an M.S. degree in Molecular Science and Nanotechnology and a Ph.D. in Engineering from Louisiana Tech University Ruston, LA, USA, respectively. Before joining the Ph.D. program at Louisiana Tech University, he graduated with an M.Sc. in Bioinformatics from Jamia Millia Islamia University, New Delhi, India. Dr. Sufian has over 14 years of teaching, research, and industry experience. He has published his research in conferences and highly reputed International journals. He has authored many chapters in the area of Artificial Intelligence/Machine Learning and blockchain/IoT. He has developed an algorithm for Face Detection, Recognition, and Emotion Recognition. He is currently in the process of developing a device that, using Biosensors, can correlate the physiology of the human body with the emotion recognition algorithm, giving us a clear measure of the amount of stress hormones in the body. Currently, he and his group have developed an ML model that predicts COVID-19 infection just from the patient's symptoms.

Dr. Jameel Ahamed has done his Doctor of Philosophy (Ph.D.) from the National Institute of Technology Srinagar, J&K (NIT Srinagar). He has completed a Bachelor of Technology (B.Tech.) from the Faculty of Engineering, Jamia Millia Islamia, New Delhi, and a Master of Technology (M.Tech.) from the National Institute of Technology, Srinagar, J&K (NIT Srinagar). Before joining the School of Technology, MANUU, Hyderabad, as an Assistant Professor, he worked as Guest Faculty in the Department of Electronics Engineering, Aligarh Muslim University, Aligarh, Uttar Pradesh for over a year. He coordinated two Faculty Development Programmes sponsored by DST and UGC. He also completed one Research Project of 01.05 Lakh. He has more than 15 research publications to his credit and delivered many invited talks. He has visited countries like the Czech Republic and the UK for conference paper presentations. He has supervised seven Master of Technology (M.Tech.) and several Bachelor of Technology (B.Tech.) and MCA research projects. His research areas include the Internet of Things, Computer Networks, Machine Learning, and Network Security.

Prof. M. A. Rizvi (Dean) obtained his Doctorate in Computer Science from Maulana Azad National Institute of Technology (MANIT) Bhopal. Dr. Rizvi has also achieved a Master's degree in Electronics and a Graduate Diploma in Computer Applications from Aligarh Muslim University, Aligarh, and a Master's of Business Administration (MBA HR) from Barkatullah University Bhopal. Dr. Rizvi has more than 29 years of experience in the field of Computer Science and Applications as a faculty (Professor and Dean) at the National Institute of Technical Teachers' Training and Research, Bhopal (NITTTR) a Government of India Institute. He has published approximately 140 research papers in reputed International Journals and International Conferences across the globe. He has published three patents and two copyrights on facial Recognition Algorithms and Computer vision-based automatic attendance calculation and updating systems. He has attended many International/National Conferences in India and abroad to present his research papers. He was invited to many International conferences as a keynote speaker, session chair, and invited talk. A book named *Computer and Communication a Practical Manual for Internet Café* for NCERT New Delhi India written by him is another feather to his cap. He has authored 10 chapters in edited books published by international publishers.

Contributors

Samra Afzal Department of Computer Science and Information Technology, School of Technology, Maulana Azad National Urdu University (Central University), Hyderabad, India

Sannasi Ganapathy Department of Computer Science and Engineering Education, National Institute of Technical Teachers' Training and Research (NITTTR), Bhopal, Madhya Pradesh, India

Elham Ghanbari Department of Computer Engineering, Yadegar-E-Imam Khomeini (RAH) Shahre Rey Branch, Islamic Azad University, Tehran, Iran

Mayuresh Gulame Department of Computer Science, School of Computing, MIT Art, Design and Technology University, Pune, India

Syed Imtiyaz Hassan Department of Computer Science and Information Technology, School of Technology, Maulana Azad National Urdu University (Central University), Hyderabad, India

Saymanov Islambek School of Mathematics and Natural Sciences, New Uzbekistan University, Tashkent, Uzbekistan;
College of Engineering, Central Asian University, Tashkent, Uzbekistan;
Applied Mathematics and Intelligent Technologies Faculty, National University of Uzbekistan, Tashkent, Uzbekistan

Sulaxan Jadhav DY Patil International University, Pune, India

Vinaya Keskar ATSS College of Business Studies and Computer Application, Pune, India

Priya Khune Department of Computer Science, School of Computing, MIT Art, Design and Technology University, Pune, India

Mohini Kumbhar Department of Computer Science, School of Computing, MIT Art, Design and Technology University, Pune, India

Vijaya Kumbhar School of Computer Studies, Sri Balaji University, Pune, India

Rakhimberdiev Kuvonchbek Digital Economy Faculty, Tashkent State University of Economics, Tashkent, Uzbekistan

C. Manimegalai Department of Computer Science and Engineering, IFET College of Engineering, Villupuram, India

Geetesh Kumar Mishra Sparklabs Diagnostics India LLP, Vadodara, Gujarat, India

Komal Munde Department of Computer Science, School of Computing, MIT Art, Design and Technology University, Pune, India

Sara Najafzadeh Department of Computer Engineering, Yadegar-E-Imam Khomeini (RAH) Shahre Rey Branch, Islamic Azad University, Tehran, Iran

Fatemeh Nasiri Department of Computer Engineering, Yadegar-E-Imam Khomeini (RAH) Shahre Rey Branch, Islamic Azad University, Tehran, Iran

M. A. Rizvi Department of Computer Science and Engineering Education, National Institute of Technical Teachers' Training and Research (NITTTR), Bhopal, Madhya Pradesh, India

Neetu Sharma Department of Applied Mathematics, Faculty of Technology and Engineering, The Maharaja Sayajirao University of Baroda, Vadodara, Gujarat, India

Mahendra Suryavanshi Department of Computer Science and Applications, MIT World Peace University, Pune, India

K. Swetha Department of Computer Science and Engineering, IFET College of Engineering, Villupuram, India

R. Thenmozhi Department of Computer Science and Engineering, IFET College of Engineering, Villupuram, India

Krishnakumar Vaithianathan Department of Computer Engineering, Karaikal Polytechnic College, Karaikal, Puducherry, India

Kanchan Wankhade Department of Computer Science, School of Computing, MIT Art, Design and Technology University, Pune, India

Pallavi Yarde Balaji Institute of Technology and Management, Sri Balaji University, Pune, India

Chapter 1
Blockchain Application in Supply Chain Management

Fatemeh Nasiri, Sara Najafzadeh, and Elham Ghanbari

Abstract This chapter explains the transformative effect of blockchain technology on traditional supply chain systems, exclusively its ability to appease inadequacy, reduce the risk of fraud, and increase transparency. Blockchain technology, centered on Distributed Ledger Technology (DLT), offers a transparent, tamper-proof, and secure, way to maintain records across the supply chain. Its applications include increasing transparency and traceability, optimizing inventory and logistics, using smart contracts to automate transactions, and inhibiting faking for brand protection. Blockchain's immutable and decentralized ledger two properties increase traceability by creating an invariable record of a product's trip. Real-time visibility of inventory lists and statuses improves anticipating, request planning, and logistics management. This leads to decreased costs and increased efficiency in warehousing, transfer paths, and the use of better resources. Smart contracts simplify the automated, secure, and transparent implementation of predefined contractual terms, leading to increased efficiency, cost reduction, and support for contractual liabilities. Blockchain is like a secure digital finger on the products in the end-to-end supply chain. So, it can fight counterfeiting and certify product originality. Although, there are several challenges with blockchain technology such as cost, privacy, scalability, regulation and standardization, transparency, and visibility. In the future, blockchain with special attention to Artificial intelligence (AI) and Internet of Things (IoT), will improve the blockchain industry, and prospect hybrid blockchain models will appear in different sections of the craft. Through new policies, innovative research, and success over challenges, stakeholders can benefit from full blockchain potential in end-to-end supply chain management and create stable, strong, and flexible supply chain management.

F. Nasiri (✉) · S. Najafzadeh · E. Ghanbari
Department of Computer Engineering, Yadegar-E-Imam Khomeini (RAH) Shahre Rey Branch, Islamic Azad University, Tehran, Iran
e-mail: fa.nasiri@iau.ac.ir

S. Najafzadeh
e-mail: sa.najafzadeh@iau.ac.ir

E. Ghanbari
e-mail: el.ghanbari@iau.ac.ir

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2025

K. Ahmad et al. (eds.), *Fostering Machine Learning and IoT for Blockchain Technology*, Transactions on Computer Systems and Networks,
https://doi.org/10.1007/978-981-96-4074-4_1

Keywords Supply chain · Blockchain · Supply chain management

1.1 Introduction to Blockchain

Initially created for Bitcoin, blockchain is a decentralized technology and data management transactions that enable individuals and firms to store and transfer value without relying on traditional mediators. Blockchain technology consists of a distributed ledger that is shared across a completely decentralized peer-to-peer network. Each node in the network takes control of a copy of this ledger. Changes to the ledger are examined and approved by each node. If a node goes inactive temporarily, it can synchronize its ledger copy from other peer nodes upon reactivation. The integrity of the ledger is preserved through a distributed consensus process, where each participating node must validate a transaction before it is written on the ledger (Tezel et al. 2021). Once recorded on the ledger, the data becomes immutable and is constantly logged in the blockchain. This data is structured into blocks, which are interconnected to form a chain through the preceding block's hash. Hash codes ensure that blockchain data remains invariable. Consequently, altering a single transaction within a block necessitates modifying all preceding blocks, a terrible challenge. The security of the blockchain amplifies as the blockchain lengthens. Unlike centralized databases, blockchain technology stores data across network nodes, increasing stability and resistance to hacking. Blockchain operates as a distributed ledger, adding records that cannot be deleted or changed without a collective agreement. The cryptographic signing of records reinforces the security of transaction data, preserving data integrity (Wan et al. 2020; Wang et al. 2019).

Blockchain is broadly affirmed for its security and safety. The three fundamental concepts in blockchain are blocks, nodes, and miners. Instead of storing data in a central location, the blockchain is duplicated and expanded across a network of computers. Each computer on the network makes up to date its blockchain to add a new block. With robust technologies like machine learning and artificial intelligence, the industry would become increasingly related to blockchain. As a relatively new and evolving technology, blockchain offers innovative applications that can lead to successful outcomes, including smooth and efficient data sharing among all important network participants. Blockchain features such as transparency and immutability can be powerful forces in the fight against bribery and corruption. Moreover, blockchain is likely to divide whole supply chains, which have several intermediaries, and replace the path consumers buy products. The effect of blockchain in industries like retail, banking, healthcare, logistics, and agriculture is digitizing, a large amount of data is captured and analyzed, and as a result, the processes are automated to make them more efficient. Blockchain technology has the potential to equip a scalable and secure data management layer for new economic models (Tezel et al. 2021; Wan et al. 2020).

The old technology of supply chain management, which is extremely based in the physical world cannot efficiently proper the changing market needs in time, and also manage the risks and costs of operations. Modern manufacturers and suppliers should invest in versatile tools and services that manage inventory, fulfill orders, and handle channel distribution effectively. Blockchain technology offers promising prospects for businesses and consumers to conduct value exchanges in real time without the need for third-party intervention (Wang et al. 2019; Zou et al. 2020).

The key characteristics of blockchain technology that are common across all blockchains include distributed resilience and control, decentralized network, transparency with pseudonymity, irreversibility of records, security and modern cryptography, and programmable logic. Blockchain technology offers several benefits, including lower transaction costs, increased speed, and efficiency in business processes, reduction in fraud, decreased systemic risk, the enablement of new business models, application streamlining, and redundancy. Some general weaknesses of blockchain technology can be explained as Scalability, efficiency and maintenance issues, regulatory and governance uncertainty, security vulnerabilities, and new attack vectors (Wang et al. 2019; Blossey et al. 2019).

1.1.1 Technical Overview of Blockchain

Blocks in a blockchain store transaction information that is recorded upon the data. Each block comprises several fields, each serving a clear purpose. The format of a block can differ across platforms and applications. However, there are some common core fields within the blocks. The infrastructure of a block and the blockchain is illustrated in Fig. 1.1. The transactions field includes data about transactions conducted on the network among various sections or involving the data itself. A block may include an "n" number of transactions, which are chosen via consensus protocols (Zou et al. 2020; Sivula et al. 2021; Thakur and Nayak 2020). The time of the block creation is stored in the timestamp field. Once a block is made and added to the blockchain, it cannot be modified. The nonce amount is computed through enormous calculations to meet a specific hash difficulty level. The hash and prior hash fields in the block warranty the chain's integrity. Even a small modification in the block's data will directly alter the hash value. Should a wicked user try to insert a block into the blockchain, they would need to re-compute the hashes and nonce values for all further blocks, checking more than 50% of the network's nodes. Transactions within a block are constructed as a Merkle tree. This tree holds the hash of each transaction at its leaves, while the higher-level nodes carry the combined hash of their respective lower-level hashes. The Merkle tree design facilitates the confirmation and reliability of personal transactions independently of others in the block. The Merkle root, which is the uppermost node of the tree, is stored in the block's header, securing the integrity and stability of all transactions on the blockchain (Thakur and Nayak 2020; Gonczol et al. 2020).

There are diverse kinds of blockchain technologies such as hybrid or consortium, public, and private, under the availability and authorizations required to connect the blockchain network. Each blockchain network has various benefits and drawbacks that fundamentally affect its ideal applications. A kind of network should be selected

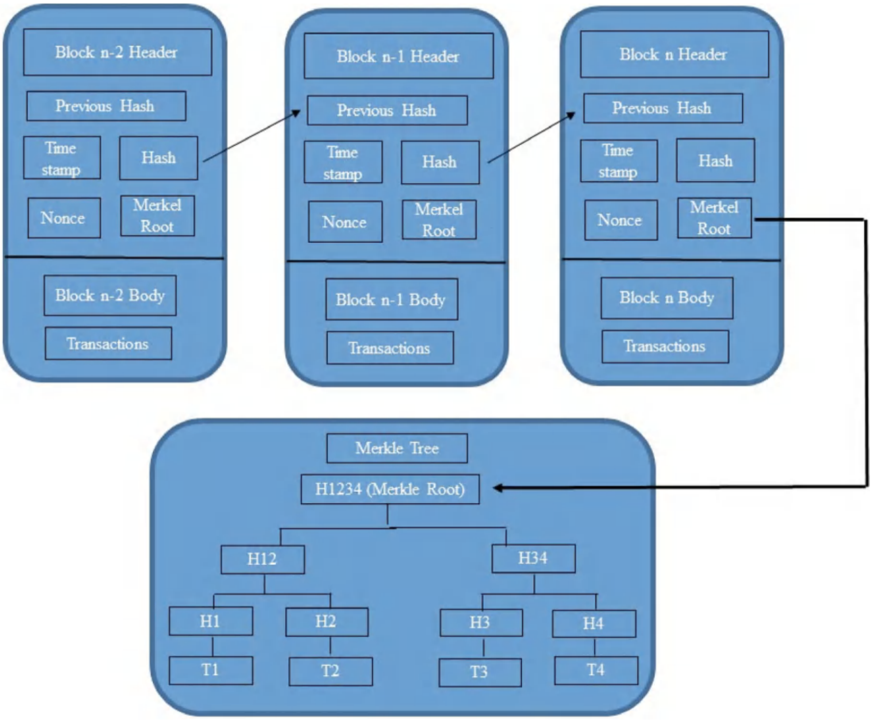


Fig. 1.1 The infrastructure of block and the blockchain

under the specific requirements of the application for which the blockchain is to be selected (Zou et al. 2020; Thakur and Nayak 2020).

A public blockchain is open for anyone to join. It's the platform where Bitcoin and other cryptocurrencies have been developed, contributing to the improvement of Distributed Ledger Technology (DLT). Within the network, there are wallet nodes, miner nodes, and full nodes, each determined by their computational power and valency. There are no restrictions on the tasks of any node. However, some businesses dislike exposing their susceptible data to the global nodes of public blockchain networks (Wan et al. 2020; Zou et al. 2020; Blossey et al. 2019).

In a private blockchain network, a trading company determines who may join the network, the types of transactions that are permitted, and the consensus algorithms to be applied. Permissioned blockchain networks use a distinct access control layer to assign specific roles and access rights within the blockchain. These networks are considered intermediate between fully private and fully public blockchains. Unlike public web solutions, permission-based blockchains certify user anonymity. A hybrid blockchain is a mix of both private and public blockchains. It permits businesses to establish a private, permission-based network besides a public, permissionless one. This hybrid system allows for controlled access to certain data while also making other data publicly available on the blockchain (Kaur et al. 2023; Rijanto 2021).

There is a mechanism in the blockchain network called consensus. A consensus mechanism is needed for all nodes of the network can agree on the new block to be added to the blockchain or updated. Various algorithms are used in blockchains to realize distributed consensus. Blockchain networks consist of plenty of nodes distributed across different locations. All nodes have the same chance to add or update their blocks in the blockchain network. Each node in the blockchain network executes smart contracts instead of on a central server. Smart contracts are compact programs that can remain in the blockchain network. When certain predefined, conditions occur, the program code is automatically executed. So, in smart contracts, no party can modify and immutable accredit the agreement situation without the others' satisfaction of the other parties. Smart conditions can be written in different languages. Some program languages utilized in smart contracts are Java, Solidity, Python, JavaScript, Go, and more. Smart contracts offer various advantages like increased speed, precision, transparency, reduced cost, and independence (Gonczol et al. 2020; Rijanto 2021).

As a review of articles showed, researchers have preferred to use permission-based blockchain systems as mentioned above because these systems prepare advantages of access control and role description. Few researchers have worked on hybrid systems which can be explored as further Spheres.

Consensus algorithms are an essential part of blockchain systems. The appropriate choice of consensus algorithms can decrease the time and cost of the network. Consensus algorithms can be summarized as Proof of authority, Proof of work, Proof of reputation, Proof of concept, Proof of importance, Kafka, Galaxy consensus, Byzantine fault tolerance, practical Byzantine fault tolerance, Proof of stake, etc. In addition, researchers will propose more types of new consensus algorithms in the next research (Blossey et al. 2019; Mukri 2018).

Smart contracts are an important part of blockchain technology to maintain system integrity, access control, and security. Most of these studies have not proposed new smart contracts, which is an important necessity for future work. There are different types of program languages for smart contracts like Solidity, JavaScript, Rust, Chain code, and Go. Solidity is the most widely used language in Ethereum because there is a huge domain future for newer languages. There are various evaluation methods to analyze proposed models. Most researchers have used performance parameters such as throughput, communication cost, latency, computation cost, transaction time, data size, and more. However, few researchers have used survey-based evaluation methods. The function of blockchain is to record different transactions in a decentralized ledger. It is precise and simple, reducing time and cost, and thus it reduces management attempts (Thakur and Nayak 2020; Kaur et al. 2023).

1.2 Evolution of Supply Chain Management

This section outlines the characteristics of the supply chain and its management across different stages. It also delves into the obstacles encountered by traditional supply chains and explores how new technology can improve management practices.

1.2.1 Traditional Supply Chain Management Challenges

A supply chain includes all entities directly or indirectly involved in complying with a customer's request. The chain comprises retailers, warehouses, transporters, suppliers, manufacturers, and customers. Within an organization, like a manufacturing firm, the supply chain consists of all operations related to fulfilling and receiving a customer order, such as operations, new product development, distribution, marketing, customer service, and finance. It is a dynamic system characterized by products, the constant flow of information, and funds across diverse stages (Gonczol et al. 2020). Figure 1.2 illustrates the supply chain stages.

Supply Chain Management (SCM) is the strategic consonance of business functions, encompassing all activities relevant to procurement, sourcing, conversion, and logistics. This management involves close cooperation with partners like suppliers, mediators, service providers of third parties, and customers. SCM combined supply and request management both within and across firms, acting as a unifying force to link essential business processes and create an agglutinate, efficient business model. This integration includes logistics, and manufacturing operations, and extends to finance, sales, marketing, sales, product design, and information technology. SCM goals are to broaden the view beyond individual organizations to include the entire supply chain, seeking to modify transparency and streamline the coordination and configuration of supply chain activities, breaking through functional and corporate limitations. Conventionally, the marketing, distribution, planning, manufacturing, and purchasing functions within a supply chain have functioned independently. Traditional management methods are deeply ingrained in a conversion or transformation view of production, in contrast to SCM, which accepts a flow view. The conventional supply chain faces numerous challenges, including a narrow perspective of the supply chain, information as it passes through each entity, a limited scope that prevents significant collaboration, distorted end-customer demand due to information distortion along the material path, and inconvenient planning cycles that cause delays and uncoordinated responses at various stages (Sivula et al. 2021; Thakur and Nayak 2020; Gonczol et al. 2020; Kaur et al. 2023; Rijanto 2021; Mukri 2018). While logistics is often seen as synonymous with the supply chain, it is just one part of it. Modern SCM systems, which are managed digitally, consist of material handling and software that support all parties involved in the creation of products or services. This includes order processing, fulfillment, and information tracking for suppliers,

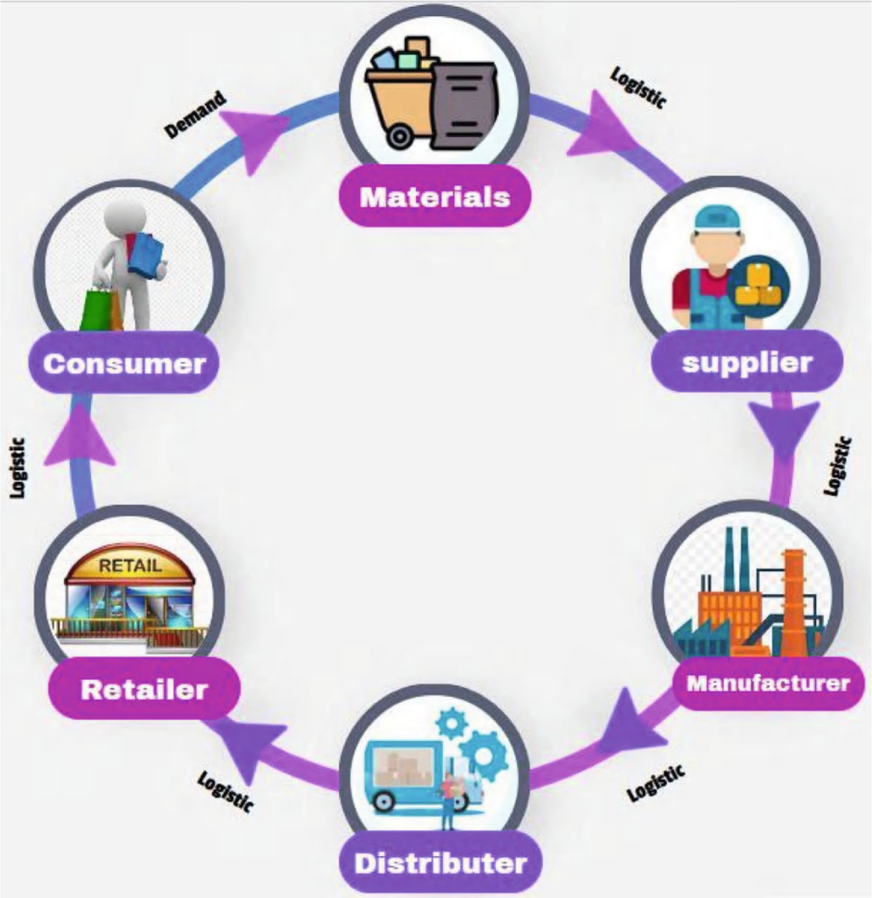


Fig. 1.2 Supply chain stages

wholesalers, manufacturers, logistics providers, transportation, and retailers (Mukri 2018).

1.2.2 *Role of Technology in Modern Supply Chain Management*

Modern supply chains have undergone significant transformations, evolving from a traditionally operational role to a distinct and strategic supply chain management function. Supply chain processes encompass a variety of logistics operations, such as scheduling, performing, and administering the impressive movement and services, storage of shipments, and related data from the point of beginning to use is essential to satisfy customer demands. Integrating and streamlining these processes can provide a competitive edge through enhanced visibility, revenue optimization, quicker inventory turnover, accelerated supply chain, and improved customer service. However, achieving these goals is challenging due to the increased complexity of supply chains. This complexity arises from the interactions among various entities located in different places, operating independently, and frequently competing to meet the requirements of their respective customers. In addition to complexities, supply chains are not only complex but also susceptible to a vast range of uncertainties and risks. These risks contain the possibility of trading partners resorting to opportunistic behaviors such as information distortion and cheating, privacy breaches, fraud, cybercrime, and challenges related to identifying counterfeit products. To address these challenges, corporate managers in different industries seek to increase supply chain management through digitalization. The digitalization of supply chains involves organizations implementing inter-organizational systems that enable collaboration and transactions with their trading associates, like key suppliers and customers, throughout their supply chains (Dursun, et al. 2022; Gurtu and Johny 2019).

The modernization of the supply chain is a significant endeavor and plays a critical role in increasing the competitiveness of different organizations. The supply chain inherently carries various risks linked to its nature. SCM faces numerous challenges driven by a range of indoor and outdoor factors. Globalization and interconnected supply chains enhance SCM convolution and risk. Other challenges arise from the continuous pursuit of increased efficiency and reduced operating costs for products. In manufacturing, shortening product lifecycles, outsourcing, adopting Just-in-Time inventory systems, optimizing machinery utilization, and consolidating suppliers are elements of business models that have brought about notable enhancements but also present significant challenges and risks to supply chain management. Various risks and challenges of SCM can be mentioned, such as sudden demand changes, lack of end-to-end visibility, obsolescence of technology, ineffective supply chain risk management, unforeseen delays, quality customer services, and supplier relationships (Rijanto 2021; Mukri 2018; Dursun, et al. 2022; Gurtu and Johny 2019; Goyat et al. 2019).

Participants in SCM face several limitations. Among these is the challenge of transparently verifying the origin and quality metrics of products, which presents an important obstacle for producers. Another limitation is the ability to track products to their final destination and assess the quality of raw materials, affecting manufacturers. Distributors face limitations due to custom tracking systems that have insufficient cooperation features, restricted certification capabilities, and trust issues. Wholesalers are hindered by the absence of trust and certification regarding the products' journey. Retailers face challenges stemming from the distrust and lack of certification of the products' route, as well as difficulties in tracking products from consumers back to wholesalers. Consumer difficulties include a lack of confidence regarding the adoption of the product concerning origin and quality, as well as compliance with specified standards and origin. Suppliers' limitation is the lack of transparency that influences the supplier's efficiency. Blockchain and new technologies provide the essential infrastructure that cutting-edge technologies require. Therefore, an increased emphasis on integrating and collaborating with technologies such as the Internet of Things (IoT), big data, Artificial Intelligence (AI), and cloud computing is important for developing sophisticated supply chain systems. The new technological framework inherently meets numerous criteria for a robust and streamlined supply chain, making it a clear selection for industries and their financial partners to adopt for supply chain management (Goyat et al. 2019; Sahoo et al. 2022; Dudczyk et al. 2024).

1.3 Blockchain in Supply Chain Management

Supply chain management encompasses the whole sales process, containing contracts, customer sales, and distribution. It aims to create a collaborative environment among different stakeholders, foster mutual trust, remove communication barriers, and ensure regular integration of the full supply network by interconnecting various companies. This integrative approach manages the whole flow of a distribution channel, from upstream activities containing people, resources, and production procedures to downstream operations. Stakeholders in the supply chain can amend total performance and create more worth for their businesses. However, multiple crucial subjects continue to challenge current supply chain management practices (Bhargava et al. 2023). The developing adoption of IoT is significantly affecting supply chain management. IoT simplifies the tracking of products, packings, and shipment containers at all stages, increasing the transparency of information across the supply chain. However, these tools and applications require concentrated scheduling and unity by a government agency, a leading enterprise, or an independent entity. Despite this, such central bodies often possess limited oversight and are unable to govern the whole supply chain due to a lack of transparency. As a result, users are often left in the dark regarding the complicated details of transactions. Additionally, many logistics entities, created by major organizations to meet their network requirements, rely on centralized regulatory authorities, like third-party logistics companies. Entities with vast operational reach and the power to manage their suppliers often face the issue of low transparency due to the many parties involved. The global nature of business, with its distributed production and different information repositories, frequently leads to information asymmetry and isolation within a large number of supply chains. Transparency is typically at a low level, and there is a lack of effective trust mechanisms among the various stakeholders. Stakeholders often find it difficult to gain a full view of all transactions and trace product origins. This challenge is especially acute for suppliers and customers who have only restricted accessibility to information all over the supply chain. Consequently, the multiplication of spurious things and quality disgraces can adversely affect the entire supply chain. This scenario may result in issues like information cheat and extortion among supply chain participants. It is significant to Build trust and ensure transparency across the supply chain, which needs the optimization of information flow. This includes gaining an all-encompassing perspective of related activities and unifying the supply chain by accepting cutting-edge technologies such as distributed ledger systems and cloud-based platforms. Through these measures, organizations can improve their performance, mitigate process risks, and achieve their business objectives. Moreover, the adoption of new technologies not only enhances business process capabilities but also bolsters regulatory compliance by reducing the burden on the central enterprise (Rijanto 2021; Mukri 2018; Dursun et al. 2022; Gurtu and Johny 2019; Goyat et al. 2019; Sahoo et al. 2022).

Blockchain technology has the potential to tackle challenges in the supply chain and support the necessary aims of supply chain management, including decreased expense, quality enhancement, increased acceleration, reliability, reduced risk, flexibility, and stability. Consequently, the supply chain needs particular consideration for innovation and transformation through blockchain technology (Dudczyk et al. 2024).

Some of the causes for applying blockchain in supply chain management include records of tamper-proof transactions, synchronized information sharing, and execution of smart contracts. Blockchain technology prepares the development of tamper-proof transaction records through a data construction that allows for the establishment of a digital ledger, which can be shared securely. Cryptography with a Public–private key is utilized to mark transactions between parties. A ‘public key’ is employed to publicly verify transactions among network entities, while the ‘private key’ allows the recipient to verify the transaction privately. The transactions are then recorded on a dispenser, invariable ledger. This rule of technology can facilitate real-time traceability and verification of product origins in the upstream supply chain, thereby bolstering the trust of downstream stakeholders in product reliability. Thus, blockchain engenders trust among suppliers and can be deployed at a relatively low cost. Information sharing and synchronization are becoming increasingly challenging due to the short life cycles of products and the lengthy lead times in production. Supply chains are thus at risk of either overcapacity from low demand or a shortage of product availability, known as the ‘bullwhip effect.’ To mitigate capacity risks, it’s crucial to decrease data asymmetry and enhance data sharing throughout the supply chain (Wang et al. 2019; Lazareva 2021). Traditional methods of sharing information or adopting an integrated Enterprise Resource Planning (ERP) system for view are often costly and impractical. Consequently, blockchain technology, founded on the peer-to-peer network principle, becomes a viable solution. In such a network, every node shares information and maintains a full ledger of historical transactions, acting as both server and client. This ensures that each node agrees on the distributed ledger’s current state, maintaining information consistency. Smart contract execution refers to a computer protocol that emulates a traditional contract. It can manage digital finance and define the rights and liabilities of the participants. When certain preconditions are satisfied, the computer system automatically executes the smart contract (Zou et al. 2020; Agarwal 2018). This process aids in facilitating contract negotiations, simplifying terms, implementing execution, and verifying the state of contract fulfillment. Consequently, actions like payments can be triggered transparently and

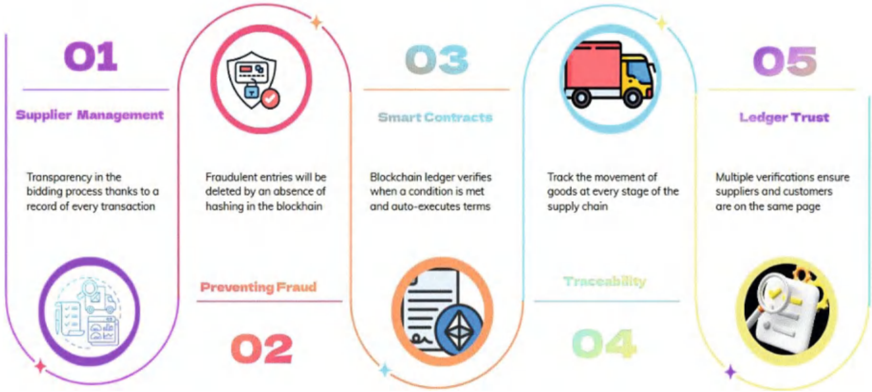

01
Supplier Management
Transparency in the bidding process thanks to a record of every transaction
Fraudulent entries will be deleted by an absence of hashing in the blockhain
Preventing Fraud
02
03
Smart Contracts
Blockchain ledger verifies when a condition is met and auto-executes terms
Track the movement of goods at every stage of the supply chain
Traceability
04
05
Ledger Trust
Multiple verifications ensure suppliers and customers are on the same page

Fig. 1.3 Implementing blockchain in the supply chain

efficiently, reducing third-party values, streamlining supply chain management, and mitigating risks. Figure 1.3 illustrates the implementation of blockchain technology in the supply chain.

In the raw material stage, blockchain allows for tracking materials from production to the end consumer, ensuring trust throughout the process. Blockchain maintains supplier trust and enhances transparency in documents and agreements. The distributed consensus of blockchain technology adds value for manufacturers, from raw material producers to suppliers. Features like proof-of-identification, smart contracts, and proof-of-location enable distributors to get certification in the distributed ledger. Blockchain enables wholesalers to verify product origins, certifications, goods transformations, and transport conditions (Agarwal 2018; Alladi et al. 2019).

Figure 1.4 illustrates blockchain effectiveness in the supply chain stages. According to the information provided, effective communication is essential for customer service. Blockchain technology can reduce the time customer service teams dedicate to processing problems. By having access to extensive data, the necessity for administrative duties to monitor or comprehend a product's status and the estimated delivery time as it proceeds via the supply chain is minimized.

The issue of budget versus results is multifaceted. Escalating gasoline and trucking expenses, fluctuating demand, modern technology, new legislation, increasing labor costs, and surging commodity prices all add to the unpredictability and intensify competition among supply chains. Blockchain can mitigate these costs by automating processes without errors. It enhances the transparency and predictability of transactions and expedites the movement of physical goods. Blockchain maintains an unalterable record of provenance, documenting all actions, movements, and the status of items at specific locations and times. Companies leverage this data to combat crime and monitor production. Additionally, it reveals strategic weaknesses, fosters sustainability, and corporate social responsibility, and opens opportunities for process reengineering (Alladi et al. 2019; Sedlmeir et al. 2022; Agrawal et al. 2021). Risk

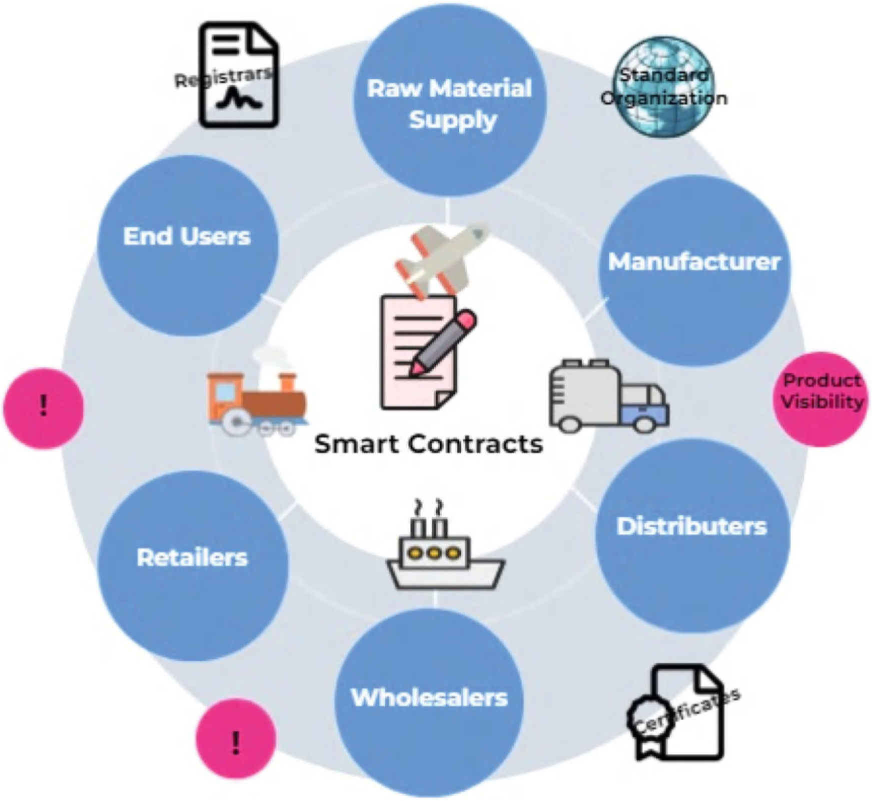


Fig. 1.4 Blockchain in supply chain stages

management is crucial for supply chain participants to enhance their resilience against disruptions in product movement. The more safeguarded they are from external risks like economic and political upheavals, the stronger their defense against internal risks such as market fluctuations, cutting-edge technology, novel or enhanced products, loan accessibility, and global sourcing activities. Blockchain technology streamlines the chain by eliminating unnecessary intermediaries and centralized services that introduce friction in terms of costs and delays and facilitates adherence to customs and regulatory standards (Bhargava, et al. 2023; Lazareva 2021).

Relationship management is another category. Suppliers and partners can optimize the product flow through the supply chain by aligning with and adhering to performance measurement standards. Mutually agreed-upon standards that ensure consistent output will foster friendly relationships between suppliers and partners. Every participant in the supply chain blockchain network can access two-way metadata about product movements. This transparency means they are informed of the goods' status as they progress through the supply chain, and suppliers disclose their sources. Lower-tier suppliers can adjust their schedules to accommodate surges in demand by having visibility into new orders (Agarwal 2018; Sedlmeir et al. 2022).

1.4 Benefits and Challenges of Blockchain in Supply Chain Management

In supply chain management, the supply chain represents a network of persons, companies, supplies, operations, and technologies that are involved in making and selling a service or product. Blockchain technology enables users throughout the supply chain to access a digital automated system that logs all changes and tracks the transfer of goods without man interposition. Each transaction or entry on the blockchain is more efficient and transparent. The system ensures that inventory does not duplicate while progressing through the chain, providing a united view and real-time updates with complete action traceability. This significantly reduces the time required for international commerce and eliminates any existing physical processes. This section will explore the advantages and challenges of executing blockchain technology in supply chain management.

1.4.1 Advantages of Blockchain in Supply Chain Management

Blockchain technology offers numerous advantages in SCM, including enhanced traceability, increased transparency, and improved efficiency. These benefits help to a more secure, reliable, and cost-effective supply chain (Dursun et al. 2022). Various benefits of blockchain technology are highlighted in SCM stages such as (Gurtu and Johny 2019; Goyat et al. 2019): Reducing delay in paperwork, minimizing courier cost, improving inventory management, identifying issues faster, improving consumer and partner trust, and Reducing fraud and error.

Delays in work supply due to paperwork can be mitigated through blockchain-based supply chain management. This approach ensures that the entire transaction history and data are stored distributive, allowing any authorized entity to access the information. The integration of blockchain into SCM enhances trust among consumers, customers, manufacturers, and suppliers. Within the blockchain ecosystem, both sellers and buyers are verified, ensuring product authenticity. Moreover, since prices are immutable, the traditional invoicing process may become obsolete. When a purchase order is logged as a block on the blockchain, it becomes an unalterable digital record. The advantages of blockchain technology in supply chain management can be summarized in several key points (Sahoo et al. 2022).

1.4.1.1 Consensus

Blockchain consensus enables stakeholders to monitor the entire supply chain process, enhancing trust in supply chain management. All features, including certification, quality, quantity, and other product details, are recorded in the consensus, thereby increasing the value of the final products. The validation of raw material quality and the verification of manufacturers' certifications contribute to greater transparency and additional value for the final product (Dursun et al. 2022; Gurtu and Johny 2019).

1.4.1.2 Distributed Ledger (Decentralization)

Blockchain operates in a decentralized fashion, meaning that no single node manages the information. Information about products, from their raw stage to the final product, is stored in a distributed manner and is publicly accessible under certain agreements. This structure mitigates the risks of data loss or single points of failure. Moreover, altering and manipulating data is challenging within a distributed ledger (Gurtu and Johny 2019; Goyat et al. 2019).

1.4.1.3 Immutability

Blockchain technology is inherently distributed, featuring a public ledger with designed access controls to determine who can access it. Authentication of each participant is verified through a decision process before they can access the ledger's data. It ensures privacy by making information visible only to authorized parties and verifies critical information during authentication. The ledger is immutable, making it resistant to manipulation or tampering (Gurtu and Johny 2019; Goyat et al. 2019; Sahoo et al. 2022).

1.4.1.4 Transparency

Blockchain technology allows all stakeholders to participate in a universal supply chain system. Its peer-to-peer nature is crafted to be robust and scalable, eliminating any single reason for failure. The distributed ledger technology is shared among stakeholders, enhancing transparency and scalability (Gurtu and Johny 2019; Goyat et al. 2019; Sahoo et al. 2022).

1.4.1.5 Shared Transaction History

Each transaction is incorporated into blocks, and each block includes a hash of the prior block in the blockchain. This hash operation maintains the integrity of the recorded information. All past transactions are compiled into blocks and distributed among various legitimate parties (Goyat et al. 2019; Sahoo et al. 2022; Dudczyk et al. 2024).

1.4.2 Challenges and Considerations

This section outlines several key challenges and considerations of executing blockchain in supply chain management.

1.4.2.1 Laws and Regulations Subjects

Blockchain lacks a unified set of legal regulations and standards for compliance. Large SCs operate multiple manufacturing facilities, each subject to its laws and regulations. Regulatory authorities must remain vigilant and continually enhance regulatory frameworks to bolster international oversight of SCs. Governments should formulate new legislation to foster the growth of innovative technologies, ensuring they are not impeded by legal barriers, particularly in the admission of blockchain-based systems. One of the foremost challenges is harmonizing Blockchain Technology (BCT) solutions with existing regulations and global compliance standards. While strict regulations may impede progress, smart contracts have the potential to codify and enforce regulations, automating SC processes and cutting costs (Dudczyk et al. 2024; Bhargava et al. 2023).

1.4.2.2 Interoperability and Standardization Subjects

Global supply chains must effectively manage their data to ensure accessibility, authenticity, availability, digitalization, integrity, privacy, protection, provenance, security, sharing, and storage. Blockchain-based storage options can address issues with cloud-based storage and enhance data availability and security. Lack of standardization has led to unclear rules for data sharing and storage between public and private blockchains, resulting in the need for new data management standards. The absence of standardization has limited blockchain interoperability. A unified set of standards is necessary to streamline interoperability in supply chains (Dudczyk et al. 2024; Bhargava et al. 2023; Lazareva 2021).

1.4.2.3 Lack of Awareness, Education, and Innovation Subjects

Many companies are not completely informed of the true potential of BCT. This lack of understanding hinders their ability to find effective solutions, as they often seek quick fixes instead of addressing underlying organizational issues. This can make it challenging for businesses to thrive due to the loss of financial resources, skills, and expertise. The unfamiliarity and lack of knowledge about blockchain adoption have caused delays and obstacles for initiatives, worsened by labor and skill shortages. A lack of innovation presents challenges for advanced industries relying on new technologies, requiring operational and logistical improvements to support critical infrastructures for global connectivity and distribution (Dudczyk et al. 2024; Lazareva 2021; Agarwal 2018).

1.4.2.4 Performance and Scalability Subjects

Performance is a critical concern in today's global market, affecting bandwidth, efficiency, latency, throughput, and scalability. IoT networks and blockchain solutions pose significant challenges. Areas ripe for future blockchain research include communication protocols for IoT devices and sensors, energy efficiency, network scaling complexity, and limited storage. Scalability, security, and stability are challenging for IoT devices on the blockchain. Risk mitigation is crucial in improving supply chain performance and fostering innovation. Latency and scalability are major performance hurdles. Response time and system latency, which increase with user numbers, create barriers to scaling. The lack of network latency provides an opportunity for future blockchain infrastructure research. Before blockchain can become a mainstream technology, issues with computational scalability, efficiency, complex data management, and blockchain maintenance need to be overcome (Dudczyk et al. 2024; Agarwal 2018; Sedlmeir et al. 2022).

1.4.2.5 Transparency and Visibility Subjects

Blockchains can be a valuable gadget in specific situations where mutual data interchange requires to be complemented by multi-stakeholder coordination, transparency, or applicability. Blockchain's transparency conflicts with corporate secret and data safekeeping policies. Moving data off the chain reduces functionality and adds complication to smart contracts. Cryptographic solutions for these challenges are not one-size-fits-all and often impractical. This tradeoff becomes evident when scaling blockchain use to more trade partners (Dudczyk et al. 2024; Alladi et al. 2019; Sedlmeir et al. 2022).

1.5 Case Studies and Examples

This section provides a concise overview of unique applications and examples of blockchain in supply chain management. While blockchain's integration into supply chains encounters various hurdles and challenges, it has notable impacts across diverse industries. As previously discussed, blockchain can affect multiple sectors, including the food industry, timber products, textiles and apparel, public healthcare systems, the shipping industry, agriculture, financial management, voting systems, and logistics. Subsequent paragraphs will discuss the implementation of blockchain in different supply chain scenarios.

Clothing Case Study: (Agrawal et al. 2021) presents a traceability framework based on blockchain for supply chains, using the textile and clothing industry as an example. It provides a detailed framework for implementing traceability in supply chains, with a focus on tracing organic cotton using a mass-balancing confirmation method. The main result of the study is a computer simulation-based illustration of network configuration and partner reaction protocols within a complicated, multi-layer supply chain, utilizing a blockchain-based traceability framework. The research demonstrates how to secure data, exchange traceability data, and establish confidence across a blockchain network using smart contracts.

Food Products Case Study: (Perboli et al. 2018) implemented the GUEST methodology in designing a use case for a European e-commerce fresh food retailer. In the solution implementation, blockchain technology is the principal resource. In this methodology, Hyperledger architecture has been used so, cryptography, consensus algorithms, and privacy can be provided for consortium needs. The acceptance of blockchain technology enhances the benefits of the different actors involved in all processes.

Varavallo et al. (2022) discussed the creation of a blockchain-based traceability platform for the Fontina PDO cheese supply chain. The data model and architecture are crafted to connect the Algorand blockchain with the database, guaranteeing transaction registration and immutability of data. Operators record all transactions within the supply chain but only transmit the JSON data to the Algorand platform during the packaging step (Varavallo et al. 2022). These decisions result in reduced energy use, reduced cost, and low environmental effects. The platform has undergone testing and validation in Aosta Valley (Italy) dairies.

The production, transport, processing, transformation, and storage of raw milk have heightened concerns regarding the authenticity of dairy products. To address these concerns, a study was conducted involving interviews with both consumers and dairy product producers. (Niya, et al. 2021) is presented as "NUTRIA" a decentralized system for tracing dairy product supply chains. The procedure was developed and executed based on dairy producers with practical observations from the Swiss dairy supply chain in collaboration. NUTRIA aims to overcome the limitations of traditional centralized supply chain tracing methods by enabling automated tracing through a blockchain-based decentralized application. The system offers confidence and clear tracing of the supply chain, which can empower the dairy value chain.

The case study in the article examines how supply chains, particularly Wal-Mart's food supply chain, can benefit from blockchain technology through collaboration with IBM Food Trust. The study analyzed Wal-Mart's annual sustainability proficiency report and external Environmental, Social, and Governance (ESG) ratings after and before the implementation of IBM Food Trust. It was found that blockchain technology enhances loss management and ensures safety, food health, and feeding within Wal-Mart's food supply chain. The findings suggest that ESG ratings could serve as a potential quantifiable stability index for further research (Park and Li 2021).

Wood Products Case Study: New blockchain technologies could improve the reliability of wood products. Blockchain technology, especially when combined with certification, has been shown to enhance trust. Certifying bodies could issue sustainable wood production certificates to forest parcel owners (Ge et al. 2017). These certificates could be registered on a blockchain, allowing forest owners to tag harvested wood with a code linked to the certificate. This code, embedded in the wood, ensures traceability to its origin and certificate, even if ownership changes. This process enables supply chain parties to verify the authenticity of the certificate. Additionally, each transfer of ownership of the timber could be recorded on the blockchain to further enhance traceability. If a certifying company discovers a forest owner engaging in illegal harvesting, they could revoke the certificate, with the revocation being noted on the blockchain. However, developing a blockchain application for timber tracking is crucial. The use of wood DNA to independently check the geographic base of timber is examined (Vlam et al. 2018). Exploring how DNA coding could interact with blockchain is interesting because of DNA's immutable nature. Understanding DNA's ability to trace the origin of wood could lead to innovative methods that combine this approach with blockchain technology and sustainable forestry certifications (Komdeur and Ingenbleek 2021).

Agriculture Case Study: Lavazza proposed integrating blockchain technology with the xFarm platform, a digital agriculture platform designed for farmers. This collaboration aims to introduce a traceable, blockchain-supported specialty coffee blend in the third quarter of 2022. The project allows consumers to track their coffee's journey from bean to cup, providing transparency about its origin and production methods (Gazzola et al. 2023).

Healthcare Case Study: The uses of blockchain in the healthcare supply chain lead to data management, transparency, response capabilities, and essential patient evaluation to transfer an efficient public health system. Some of the uses of blockchain technology in the health care supply chain include Electronic Health Records, Decentralization, Pharma Supply Chain, Telehealth and Telemedicine, Managing financial Reports in hospitals, Use of blockchain in COVID-19, Remote Patient Monitoring, Digital Health Services, Biomedical education and research, Health data analysis, Health Insurance Claim, Validation (Sahu et al. 2024). There are several practical examples mentioned in the next paragraphs.

The solution is being developed on the Ethereum blockchain using the Truffle framework for writing smart contracts in Solidity. Ganache is used to provide a local Ethereum blockchain. Metamask facilitates transactions. Manufacturers add pre-approved medicine, and wholesalers purchase medicine by transferring funds, changing the medicine's status to "Purchased by Wholesaler and ForSale." At the last level, distributors and wholesalers can buy medicine from the wholesaler and initiate a 'purchase medicine' event, changing the medicine's status. Similarly, pharmacies can acquire medicine from the distributor, and then customers can purchase medicine from pharmacies. Additionally, customers can track and trace medicine using the medicine ID or an available barcode (Bandhu et al. 2023).

Emerging health technologies like wearables, IoT, and mobile apps are transforming the medical field. These devices monitor patient vital signs, store data securely, and analyze in real time. Privacy and security are concerns. A new healthcare paradigm, Secured Mobile-Enabled Assisting Device for Diabetics (SMEAD), aims to aid diabetic patients by using wearables to monitor various parameters and a MEDIBOX for medication reminders. Blockchain technology ensures data security and access for doctors. In emergencies, alerts are sent to caregivers via social networks, potentially preventing severe complications. SMEAD system facilitates data storage on the Ethereum-based blockchain system for millions of patients. Real-time analysis supports a withness-based medicine system while addressing security and privacy improvements and can remote patient monitoring (Saravanan et al. 2017; Elangovan et al. 2022).

In reference (Nguyen et al. 2021), BEdgeHealth is introduced as a new decentralized health architecture that leverages blockchain technology and Mobile Edge Computing (MEC) to offload and share health data across distributed medical center networks. This privacy-conscious data offloading approach allows mobile devices to offload IoMT (Internet of Medical Things) health data to nearby MEC servers considering system limitations. Additionally, a data-sharing layout is presented that utilizes blockchain and smart contracts to facilitate safe data substitution among healthcare users in various medical centers. To manage access, an Access Control Smart Contract (ACSC) is developed for decentralized user confirmation at the network border, ensuring authentication reliability and reduced network latency without the need for a central authority. The effectiveness of the BEdgeHealth could be mentioned such as lessening time latency, energy utilization, and improved memory usage.

Robomed (Ahmad et al. 2021) is a network of clinical organizations governed by smart contracts on the Ethereum blockchain. Its goal is to provide efficient medical services with a focus on patient value. The Robomed Electronic Health Care (EHR) enables healthcare organizations to self-manage within the network through Ethereum smart contracts. Key features include real-time patient interaction monitoring, decision support for medical staff, access rights management, health specialist scheduling, patient health analysis via charts, and telemedicine consulting services. Patients can use the Robomed mobile app for telemedicine consultations, appointment management, and consent contract terms during EHR sharing with clinics. Smart contracts allow tracking and validation of patient health outcomes and ensure adherence to value-based clinical guidelines. The RBM token is recognized as a payment method across the Robomed network (Network 2017; Hang et al. 2019).

Finance Case Study: in (Keller 2018; Thakur 2023) Batavia, a cosmopolitan commerce finance platform is based on the blockchain improved by the cooperation of IBM and five banks (Bank of Montreal (BMO), CaixaBank, UBS, Erste Group, and Commerzbank). This platform facilitates access to different organizations around the world. Therefore, Bativa expected to transform slow paper-based processes to digitize and speed up.

In reference (Rijanto 2021), several blockchain projects implemented in Supply Chain Finance (SCF) in different countries are mentioned. Most of them aim to

Table 1.1 Summary of blockchain project in supply chain finance (Rijanto 2021)

Blockchain Project	Description
Skuchain	Buyers and sections relevant to the supply chain are given access to firm preparation and bill of goods control
ChainNova	Invoice traceability, and L/C, Waybill
MarcoPolo	Secure, risk reduction, accounting, personality, automated, confirmation, tracking, accessible finance, invoicing, pay warranty, and divided
Geora	Smart contracts, unsegregated, IoT, asset-backed wealth, and trusted documents
Ecomchain	Digital credit documents, inquiries, pays, asset emission, pricing inventory, and fiscal asset transactions
Cargo	Intelligent waybill, a document for universal business

address issues such as digitizing records, speeding up transactions, enabling traceability, enhancing security, ensuring validation, and complying with regulations. Some of the project's names are such as Cargo, ChainNova, ecomchain, Geora, Skuchain, and MarcoPolo. Each of these SCFs has unique features related to auditing capabilities, risk reduction, and alternative funding. In Table 1.1 some of the features of blockchain Project in SCF are shown.

The Hyperledger Besu platform (Shahrukh et al. 2023) handles financial transactions with minimal computational load. It offers a promising solution for enhancing transparency and efficiency while mitigating security risks.

Fishing sector Case Study: In Proof of Concept (POC) in (Hutchins and Sutherland 2008) blockchain technology is utilized to trace the journey of seafood from the point of catch to consumption, improving sustainability in the fishing industry's supply chain (from bait to plate). Developers created an Application Programming Interface (API) that records authenticated transactions using blockchain technology, integrating various data types and sources to create digital passports. Users can upload documents, digitally encoded and added to the blockchain, resulting in a permanent record of relevant information throughout the seafood's lifecycle (Haughton et al. 2022).

1.6 Future Trends in Blockchain in Supply Chain

The important implications of blockchain technology in supply chain management are the benefits of privacy, security, and distribution in supply chain participants. Future works focus on the recognition of obstacles to adoption and improving tactics to persuade more users to accept blockchain in supply chain management. Generally, future efforts can be grouped into three areas: combination blockchain with IoT and AI, seeking hybrid blockchain models, and industry-special blockchain solutions, which will be further elaborated upon (Hassan et al. 2023).

Supply chain processes' transparency and traceability will increase with IOT combined with blockchain. Also, combining AI with blockchain improves making decisions in real time. When placed next to blockchain, IoT and AI can revolutionize supply chain management (Altekar 2023). Due to AI's capacity for analyzing big data sets and blockchain's robustness in secure data storage and access, AI can foresee market disruptions and shifts in demand, enabling informed decision-making. Consequently, businesses can remain proactive and make the best use of opportunities. Artificial intelligence has the power to revolutionize production processes, improve inventory management, and significantly enhance overall flexibility within supply chain operations. For instance, when AI algorithms combined with blockchain, can analyze data about transportation logistics and determine the most efficient transportation route (Anamu et al. 2023).

When data is recorded by IoT devices or smart sensors on the blockchain, a transparent ledger is created. This ledger is extremely helpful for improving logistics and inventory management. It allows for the tracking of goods across the entire supply chain, creating a tamper-free and secure system. By monitoring goods throughout their journey in the supply chain, any disruptions and delays can be identified promptly, and unforeseen incidents can be prevented, ultimately enhancing supply chain management (Rejeb et al. 2019).

The future of blockchain technology is focused on a significant evolution in providing solutions to change and replace common methods. The blockchain solutions offered align with addressing the needs and challenges of various industries. The potential of blockchain technology resides in the decentralized ledger systems, ensuring the transparency, security, and validity of transactions. The financial sector is making significant progress in terms of loans, remittances, and investments with the help of blockchain (Petrović 2022). By comprehending the complexities and challenges in different industry sectors such as pharmaceuticals, healthcare, agriculture, manufacturing, textile, wood, and shipping industries, standardized platforms are provided. Blockchain-standardized platforms in the industry offer a transparent and auditable history, addressing challenges in specific industries. Challenges such as interoperability, standardization, and initial adoption costs need to be considered in each industry. Each supply chain has its complexities, and an industry-specific blockchain solution can optimize processes and enhance supply chain management (Shahrukh et al. 2023; Oriekhoe et al. 2024).

VeChain (Manolache et al. 2022) stands as a remarkable example of how blockchain technology can be harnessed to implement industry-specific solutions. Vechain blockchain solution helps consumers detect the authenticity of lux products. RFID tags and QR codes prevent counterfeiting lux products. To adopt tailored solutions, collaboration between industry stakeholders, technology providers, and regulatory bodies is necessary (Oriekhoe et al. 2024).

Hybrid blockchain offers a solution that mixes the advantages of private and public blockchains. It aims to address the needs of stakeholders in the supply chain. Public blockchains, such as Bitcoin, offer immutability, transparency, and security through distributed consensus mechanisms (Shahrukh et al. 2023). However, they may face scalability issues, leading to transaction delays. Conversely, private blockchains offer restricted access control and scalability, prioritizing participants' privacy. Hybrid blockchain models provide benefits such as scalability, interoperability, and flexibility across different platforms. Hybrid models utilize private blockchains to manage confidential data. Hybrid models facilitate collaboration between private and public blockchains without compromising data security or privacy. This is an important feature in hybrid models to interact efficiently between suppliers, manufacturers, and distributors. Implementation of hybrid blockchain models in various industries facilitates transparency and traceability and Intellectual property protection is provided. These cause challenges and standardization of protocols in the industry. This property highlights the importance of hybrid models in efficiently connecting suppliers, manufacturers, and distributors. Implementing hybrid blockchain models in different industries promotes transparency, traceability, and intellectual property protection. However, hybrid blockchain also encounters challenges and creates standard protocols among the industry sectors (Oriekhoe et al. 2024; Cui et al. 2020). Smart contracts can revolutionize the whole of the supply chain sectors. Smart contracts supervise how contracts are executed to reinforce trust, automation, transparent and traceable supply chain. However, realizing blockchain's potential requires collaboration between businesses, regulators, and technologists to shape a future where blockchain is necessary for improving global supply chains (Oriekhoe et al. 2024).

1.7 Conclusion

The supply chain is a complex network that comprises several sectors like retailers, wholesalers, distributors, manufacturers, and suppliers. Blockchain technology can provide various benefits to supply chain management such as decreased cost, improved efficiency, traceability, enhanced security, and increased transparency. Blockchain technology addresses the challenges of traditional supply chains such as tampering, inefficiency, and fraud. Blockchain capabilities such as smart contracts, inventory optimization, traceability, and counterfeit prevention improve fostering trust and ensure product originality. Efficiency improvements and cost savings are realized through blockchain platforms that provide real-time inventory tracking, execute automated payments via smart contracts, and enhance logistics optimization. Gains and data analysis are reinforced by the marriage of IoT and AI with blockchain technology (Hassan et al. 2023). So, it enhances the flexibility of the supply chain. Successful blockchain implementation needs to foster collaborations between partners in various industries, funding professional IT workers and infrastructure, data standardization, and rules of government. Despite challenges such as scalability, cost, and privacy, blockchain solutions are tailored to the needs of the industry sector. Each sector, such as healthcare, agriculture, finance, shipping, and food, has its unique standards and solutions. Hybrid blockchain models could ensure data privacy when needed to improve flexibility for different supply chains soon. Research in the blockchain is in its early steps. Utilizable and customizable blockchain needs industry-oriented research should address several challenges including scalability, personal data protection, cost, and governmental regulations (Alladi et al. 2019; Thakur 2023; Hassan et al. 2023; Oriekhoe et al. 2024).

References

Agarwal S 2018) Blockchain technology in supply chain and logistics. Dissertation, Massachusetts Institute of Technology

Agrawal TK et al (2021) Blockchain-based framework for supply chain traceability: a case example of textile and clothing industry. Comput & Ind Eng 154:107130

Ahmad RW et al (2021) The role of blockchain technology in telehealth and telemedicine. Int J Med Inf 148:104399

Alladi T et al (2019) Blockchain applications for industry 4.0 and industrial IoT: a review. IEEE Access 7:176935–176951

Altekar RV (2023) Supply chain management: concepts and cases. PHI Learning Pvt. Ltd.

Anamu US et al (2023) Fundamental design strategies for advancing the development of high entropy alloys for thermo-mechanical application: a critical review. J Mater Res Technol

Bandhu KC et al (2023) Making drug supply chain secure traceable and efficient: a blockchain and smart contract based implementation. Multim Tools Appl 82(15):23541–23568

Bhargava DVD et al (2023) A review of blockchain technology in different sectors: challenges and solutions. In: 2023 4th international conference on signal processing and communication (ICSPC). IEEE

Blossey G, Eisenhardt J, Hahn G (2019) Blockchain technology in supply chain management: an application perspective

Cui Z et al (2020) A hybrid blockchain-based identity authentication scheme for multi-WSN. IEEE Trans Serv Comput 13(2):241–251

Dudczyk P, Dunston J, Crosby GV (2024) Blockchain technology for global supply chain management: a survey of applications, challenges, opportunities & implications. IEEE Access

Dursun T et al (2022) Blockchain technology for supply chain management. In: Industrial engineering in the internet-of-things world: selected papers from the virtual global joint conference on industrial engineering and its application areas, GJCIE 2020, 14–15 August 2020. Springer International Publishing

Elangovan D et al (2022) The use of blockchain technology in the health care sector: systematic review. JMIR Med Inform 10(1):e17278

Gazzola P et al (2023) Using the transparency of supply chain powered by blockchain to improve sustainability relationships with stakeholders in the food sector: the case study of Lavazza. Sustainability 15(10):7884

Ge L et al (2017) Blockchain for agriculture and food: findings from the pilot study. No. 2017-112. Wageningen Economic Research

Gonczol P et al (2020) Blockchain implementations and use cases for supply chains-a survey. IEEE Access 8:11856–11871

Goyat R et al (2019) Implications of blockchain technology in supply chain management. J Syst Manag Sci 9(3):92–103

Gurtu A, Johny J (2019) Potential of blockchain technology in supply chain management: a literature review. Int J Phys Distrib Logist Manag 49(9):881–900

Hang L, Choi E, Kim D-H (2019) A novel EMR integrity management based on a medical blockchain platform in hospital. Electronics 8(4):467

Hassan DK, Metawee AK, Hassan B (2023) Blockchain technology in supply chain management: a review of business applications and future directions. Am J Bus Oper Res 1(2):60

Haughton O et al (2022) Evaluating the integration of blockchain technologies in supply chain management: a case study of sustainable fishing. In: 2022 international conference on computing, networking, telecommunications & engineering sciences applications (CoNTESA). IEEE

Hutchins MJ, Sutherland JW (2008) An exploration of measures of social sustainability and their application to supply chain decisions. J Clean Prod 16(15):1688–1698

Kaur A, Bansal S, Dattana V (2023) Blockchain in healthcare: a systematic review and future perspectives. In: Deep learning for healthcare decision making, pp 211–243.

Keller F (2018) Blockchain-based Batavia platform set to rewire global trade finance. IBM Blockchain Blog, Blockchain Pulse

Komdeur EFM, Ingenbleek PTM (2021) The potential of blockchain technology in procuring sustainable timber products. Int Wood Prod J 12(4):249–257

Lazareva V (2021) Blockchain technology in the supply chain

Manolache MA, Manolache S, Tapus N (2022) Decision making using the blockchain proof of authority consensus. Procedia Comput Sci 199:580–588

Mukri B (2018) Blockchain technology in supply chain management: a review. Int Res J Eng Technol 5(6):2497–2500

Network R (2017) Initial coin offering, white paper, robomed Network. Inc., Rusia

Nguyen DC et al (2021) BEdgeHealth: a decentralized architecture for edge-based IoMT networks using blockchain. IEEE Internet of Things J 8(14):11743–11757

Niya SR et al (2021) A blockchain-based supply chain tracing for the Swiss dairy use case. In: 2020 2nd international conference on societal automation (SA). IEEE

Oriekhoe OI et al (2024) Blockchain technology in supply chain management: a comprehensive review. Int J Manag & Entrep Res 6(1):150–166

Oriekhoe OI et al (2024) Blockchain in supply chain management: a review of efficiency, transparency, and innovation. Int J Sci Res Arch 11(1):173–181

Park A, Li H (2021) The effect of blockchain technology on supply chain sustainability performances. Sustainability 13(4):1726

Perboli G, Musso S, Rosano M (2018) Blockchain in logistics and supply chain: a lean approach for designing real-world use cases. IEEE Access 6:62018–62028

Petrović EK et al (2022) Blockchain for supply chain ledgers: tracking toxicity information of construction materials. In: Blockchain for construction. Springer Nature Singapore, Singapore, pp 89–111

Rankhambe BP, Khanuja HK (2019) A comparative analysis of blockchain platforms–Bitcoin and Ethereum. In: 2019 5th international conference on computing, communication, control, and automation (ICCUBEA). IEEE

Rejeb A, Keogh JG, Treiblmaier H (2019) Leveraging the internet of things and blockchain technology in supply chain management. Future Internet 11(7):161

Rijanto A (2021) Blockchain technology adoption in supply chain finance. J Theor Appl Electron Commer Res 16(7):3078–3098

Sahoo S et al (2022) Blockchain for sustainable supply chain management: trends and ways forward. Electron Commer Res 24:1–56

Sahu H, Choudhari S, Chakole S (2024) The use of blockchain technology in public health: lessonslearned. Cureus 16(6):e63198. https://doi.org/10.7759/cureus.63198. Online publication date:26 June 2024

Saravanan M et al (2017) SMEAD: a secured mobile enabled assisting device for diabetics monitoring. In: 2017 IEEE international conference on advanced networks and telecommunications systems (ANTS). IEEE

Sedlmeir J et al (2022) The transparency challenge of blockchain in organizations. Electron Mark 32(3):1779–1794

Shahrukh H, Raisul Md, Rahman MdT, Mansoor N (2023) A new paradigm in blockchain-based financial aid distribution. In: World conference on information systems for business management. Springer Nature Singapore, Singapore

Sivula A, Shamsuzzoha A, Helo P (2021) Requirements for blockchain technology in supply chain management: an exploratory case study

Tezel A et al (2021) Insights into blockchain implementation in construction: models for supply chain management. J Manag Eng 37(4):04021038

Thakur A (2023) Market trends and analysis of blockchain technology in the supply chain. Front Blockchain 6:1142599

Thakur D, Nayak MM (2020) A comprehensive study on block chain technology in supply-chain management. Int J Electr Eng Technol (IJEET)

Varavallo G et al (2022) Traceability platform based on green blockchain: an application case study in dairy supply chain. Sustainability 14:3321

Varavallo G et al (2022) Traceability platform based on green blockchain: an application case study in the dairy supply chain. Sustainability 14(6):3321

Vlam M et al (2018) Developing forensic tools for an African timber: regional origin is revealed by genetic characteristics, but not by isotopic signature. Biol Conserv 220:262–271

Wan PK, Huang L, Holtskog H (2020) Blockchain-enabled information sharing within a supply chain: a systematic literature review. IEEE Access 8:49645–49656

Wang Y et al (2019) Making sense of blockchain technology: How will it transform supply chains? Int J Prod Econ 211:221–236

Zou Y et al (2020) Focus on blockchain: a comprehensive survey on academic and application. IEEE Access 8:187182–187201

Chapter 2
Transformation of the Banking Sector with Blockchain Technology

Pallavi Yarde, Vijaya Kumbhar, Sulaxan Jadhav, Mahendra Suryavanshi, and Vinaya Keskar

Abstract Blockchain technology enhances security, transparency, and productivity in financial services. This chapter examines how blockchain, paired with the Internet of Things (IoT) and Artificial Intelligence (AI), is reforming the financial industry and enhancing a safe and linked smart financial service sector. Blockchain's dispersed and tamper-resistant capabilities, when paired with AI and IoT, have the potential to change crucial financial processes, aggregate confidence, reduce costs, and improve the end-user experience. The chapter reviews blockchain, its role in finance, and how IoT and AI contribute to financial innovation. It then analyzes the synergy between IoT, AI, and blockchain in the banking sector, exhibiting the potential benefits of combining this expertise for more efficiency. The chapter delves into ample financial applications of blockchain, such as cross-border payments, stock trading, smart contracts, digital proof of identity, authentication, and cryptocurrencies like Bitcoin and Ethereum. Asset tokenization, supply chain financing, trade finance, Decentralised Finance (DeFi), regulatory compliance, fraud protection, peer-to-peer lending, insurance claim processing, and Initial Coin Offerings (ICOs) are all referred. Furthermore, elements such as clearance and agreement systems, syndicated loans, risk management, and loyalty programs are addressed to prove blockchain's widespread influence on financial services. The chapter also examines research gaps in blockchain applications for the banking sector, highlighting the need for improved

P. Yarde (✉)
Balaji Institute of Technology and Management, Sri Balaji University, Pune, India
e-mail: pallavi.yarde@bitmpune.edu.in

V. Kumbhar
School of Computer Studies, Sri Balaji University, Pune, India

S. Jadhav
DY Patil International University, Pune, India
e-mail: sulaxan.jadhav@dypiu.ac.in

M. Suryavanshi
Department of Computer Science and Applications, MIT World Peace University, Pune, India

V. Keskar
ATSS College of Business Studies and Computer Application, Pune, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2025

K. Ahmad et al. (eds.), *Fostering Machine Learning and IoT for Blockchain Technology*,
Transactions on Computer Systems and Networks,
https://doi.org/10.1007/978-981-96-4074-4_2

solutions to difficulties. Additionally, integrating IoT and AI with blockchain is studied, offering perceptions on how these technologies work together to improve financial services. Real-world case studies are run to determine practical implementations. The chapter also reviews unresolved concerns and future research prospects for increasing blockchain's position in finance, accenting the technology's endless progress and intact potential. Finally, recommendations are suggested to improve the use and effectiveness of blockchain, IoT, and AI in banking. The chapter rubs by creating significant issues, presenting a thorough education of how blockchain might alter the financial sector, and outlining prospects for study and practical application.

2.1 Introduction

Blockchain is a decentralized, distributed ledger that records transactions across multiple computers so that the registered transaction cannot be altered retroactively. While blockchain was initially proposed for Bitcoin as its underlying technology, it has pretty evolved away from its original purpose of cryptocurrency as it has become a transformative technology in sectors ranging from financial services to healthcare and supply chain management (Nakamoto 2008).

This technology relies on a network of participants, sometimes called nodes, which maintain and validate a ledger. Each transaction collected into a block is added to a chain of previously executed transactions to form a blockchain. The blockchain contrasts with the central systems in that it has an element of being less trusted. Here, consensus is through algorithms either proof of work or stake. This decentralization brings security and transparency since any interference into the blockchain is very unlikely without taking control of the majority share of the computing powers of the network known as a "51% attack" (Nakamoto 2008).

Some other advantages of blockchain technology for the financial world include increased security, cost savings, and the possibility of real-time settlement. Another attractive application area is in response to central banks' challenge to digital currencies. For example, the Bank of England and the People's Bank of China have initiated efforts to collaborate on their respective notations on CBDCs with blockchain to make available an efficient and secure mode for executing financial transactions (Bank of England 2020; People's Bank of China 2021).

Another of the best-known applications of blockchains is smart contracts. These are basically programs that spell out the actual terms of the agreement directly into code. Some platforms, such as Ethereum, support this, and it's transforming the way transactions are conducted—automating the settlement of agreements without the need for an intermediary (Ethereum Foundation 2021a, b).

In brief, blockchain can solve issues in the financial and banking sectors, such as fraud, inefficient payment systems, and delays in cross-border transactions in business-to-consumer contexts. In real-world applications, Ripple can use blockchain-based payment solutions offered by leading corporate clients such as

Santander and American Express to deliver faster and safer cross-border payments (Ripple 2020).

The blockchain is now ready to transform not just cryptocurrency but the whole financial ecosystem into truer, decentralized, and safer financial services.

2.1.1 Overview of Blockchain in Banking

Blockchain technology has revolutionized the face of banks, addressing prolonged inefficiencies and security vulnerabilities associated with traditional banking systems. Additionally, although banks always employ central systems, these systems are vulnerable to delay, a high cost of transaction, and fraud susceptibility. Blockchain presents a decentralized, transparent, and secure alternative to transform many aspects of banks' operations (Nakamoto 2008). Cross-border payments are one of the most revolutionary uses of blockchain technology in banking. Traditionally, charges and complications are associated with a multiple intermedial chain in settlement times. However, blockchain technology eliminates the middleman since it is purely peer-to-peer transactions within a decentralized approach.

For example, Ripple's payment product has been seen as an opportunity for leading banks such as Santander and Standard Chartered to make the most of even improving fast and efficient cross-border transactions. Ripple allows real-time gross settlement. Costs and settlement times can drastically reduce from days to seconds (Ripple 2020).

Blockchain is another field in which digital identity verification revolutionizes the bank sector. Know Your Customer (KYC) is a vital banking practice meant to protect a bank from fraud, money laundering, or financing of terrorism. The present KYC procedures involve time-consuming and resource-consuming processes. Blockchain introduces a safe and non-amendable framework for digital identity so that customers' information regarding verification may be safely stored and shared across financial institutions, thereby saving duplication and improving compliance efficiency.

This system is fast not only in the onboarding process for customers but also in reducing the bank's operational cost (BIS 2017). Blockchain is changing credit platforms and lending systems under decentralized finance, or DeFi for short. Based on an underlying peer-to-peer infrastructure, the old banking models still work with some intermediaries prolonging the process with higher interest rates, and people cannot access credit, especially those more underserved populations. Blockchain-based DeFi enables a peer-to-peer lending environment where borrowers interact directly with lenders.

The blockchain contains intelligent contracts that can automatically release loans upon repayment, given that the predefined conditions are met. Such decentralization leads to lower costs, greater access to credit, and more transparent lending processes (Ethereum Foundation 2021a, b). The second major innovation of banks is in issuing and managing digital currency: blockchain. All central banks, from the People's Bank of China to the European Central Bank, are working on the concept called

Central Bank Digital Currency, or CBDC, which will be founded upon blockchain technology.

CBDCs facilitate both retail and wholesale payment, enabling financial institutions and governments to issue and make digital money safely, cheaply, and efficiently. The Chinese Central Bank initiated test trials for its digital yuan in 2020 and is currently working on overhauling the entire banking system with a safer alternative to Bitcoin and other cryptocurrencies (People's Bank of China 2021).

In a nutshell, blockchain revolutionizes the banking sector with developments in transaction efficiency, operational cost reduction, security enhancement, and new avenues of innovation. As banks continue to explore this subject, blockchain will form an integral part of future trends in global banking.

2.1.2 Significance of IoT in Banking

The IoT is revolutionizing banks: it enhances their operational efficiency, strengthens security measures, and improves customer experiences. The Internet of Things is defined as a network of devices and sensors capable of communicating and exchanging data in real time. Several advancements have been made in the manner in which banks interact with customers, manage assets, or even protect against fraud.

The most common application of IoT in banks would probably be its **connected devices**, resulting in higher **customer engagement**. The former example includes wearables-smartwatches plus fitness tracking combined with the Internet, enabling a user to speak into their bank account balance or transfer cash in a manner where that's done in real time, no logging into a computer or visiting a branch. The features of mobile banking applications enable banks to be linked to IoT devices, enabling seamless, convenient banking. This factor contributes to better customer satisfaction and propels the sector's digital transformation (Zhang et al. 2016; Zhao et al. 2018; Zohar 2015; Zcash 2021; Winding Tree 2018; World Bank 2020; Yearn.Finance 2021).

Detection and prevention of fraud also form an important part of IoT. Banks can detect customer behavior patterns through technology and record fraudulent transactions in real time. For instance, if a transaction occurs from an unknown location or its spending pattern does not conform to the user's habitual pattern. The IoT sensors will alert or freeze the transaction. This monitoring is time-based and increases security; by this, banks help reduce fraud and protect customer data. Biometric IoT devices like fingerprint or face recognition keep improving the safety of banking systems (Deloitte 2020).

IoT in asset management will allow banks to track and follow up on their physical assets, such as ATMs, cash dispensers, and other critical infrastructures. There is a monitoring of performance, detection of malfunctions, and probably failure prediction before an accident occurs. This ability allows banks to do predictive maintenance, hence lowering downtime and minimizing repair charges. For instance, assume that the ATM sensor determines that the cash or the hardware at the ATM has run low.

This is when the bank can notify the technician to come and fix the problem (IBM Research 2021).

IoT contributes to the banks' supply **chain financing** and **collateral management**. The fact is that real-time tracking of goods and assets based on IoT sensors enables banks to evaluate any collateral better than businesses provide for lenders. Consequently, it gives them more effortless flexibility in providing loans and financing in various sectors, with priority in the agricultural, manufacturing, and logistics areas. For example, networked sensors can sense the state of perishable commodities or even monitor shipments in transport, thus offering banks a lot of insight to assess risks and then lend appropriately (PwC 2020).

The most famous example of adoption in banking through the IoT is **contactless payments**. Thanks to the enablement of payment devices through IoT, the entire list of wearables, from smartwatches and even smartphones, allows customers to make transactions safer and faster. They are trendy and can be an alternative to traditional cash or card-based payments. For instance, the NFC technology incorporated into IoT equipment enables consumers to conduct a payment by just tapping their device at the point-of-sale terminal, which incidentally is faster and more secure in their method of processing a transaction (Capgemini , 2021a, b, c).

This can revolutionize the banking business not only by improving the customer experience, simplifying the processing cycle, and enhancing security but also by deepening the meaning of the term IoT in banking as the ecosystem expands.

2.1.3 Importance of AI in Banking

AI is one of the fastest transformers, giving a new shape to the banking sector; it automates many processes, enhances decision-making, and improves customer services. With real-time analysis of such a vast amount of data, AI channels provide the weapons with which a bank can smoothen its operations, control risk, and offer more personalized services.

The **chatbots** and **virtual assistants** will be used in the banking sector to **upgrade customer service enabled by AI**. Fundamental to their work, bank institutions entirely rely on AI-based chatbots to process routine customer queries and transactions by offering personalized and efficient financial advice. Interaction with the customer through Natural Language Processing allows faster and more seamless resolutions. For instance, Bank of America's AI-powered virtual assistant Erica helps clients pay bills, check their balances, and manage accounts. As much as AI can provide 24/7 services, it still saves on costs while increasing customer satisfaction.

One of the most critical applications for AI in banking is related to **fraud detection and prevention**. Machine learning algorithms by AI analyze millions of transactions to spot unusual patterns or anomalies signaling possibly fraudulent activity. The AI system can immediately alert a bank to suspicious transactions, thus minimizing loss. For instance, an account is suspicious when a previous transaction is in a foreign location. Moreover, the cardholder's phone may be detected in another country. AI systems can send a block request for the transaction to prevent fraud immediately. As AI can learn from patterns and develop over time, it has become unusually effective in detecting new methods of fraud (PwC 2019).

AI also reshapes **risk management**. In the traditional approach, most risk analyses are based on historical data, whereas AI brings this predictive capability through natural streams of data analysis. For instance, AI systems can be designed to monitor borrowers' credit histories constantly and be abreast of market trends and financial behaviors that might change the profile dynamically. This would allow banks to make better lending decisions and manage credit better. Banks may further scrutinize loan applications by adopting AI-based credit scoring models and alternative information on the borrower's payment history or even social media usage (Deloitte 2020).

In **investment and wealth management**, AI is an increasingly important component through **robo-advisors** and **algorithmic trading**. Robo-advisors utilize AI to help automate investment strategies based on the individual's financial goals, risk tolerance, and market conditions. These systems offer low-cost investment advice and portfolio management to a far greater range of customers than before because they democratize access to financial services. Another use is in high-frequency trading. These algorithms are taking the extensive data set and executing trades in milliseconds. That is better done by AI than human traders do (Capgemini 2021a, b, c).

AI is also redefining the concept of the nature of personalized banking services. Because with customer transaction histories, spending habits, and lifestyle preferences, AI can deliver highly customized services. For example, in terms of savings plans, tailored credit options, or investment portfolios along specific lines that cater to their individual needs and financial aspirations, AI-based systems can well advise an individual. This level of personalization ultimately results in great customer loyalty and engagement (McKinsey Company 2020).

Indeed, AI has improved compliance and regulatory reporting in the banking sectors. The regulation is complex, so the entire industry must always comply with AML and KYC requirements. AI systems may check for compliance, monitor transactions in real time for suspicious activities, and produce reports in real time to regulatory bodies. It helps the banks escape heavy fines and become more transparent (IBM Research 2021).

To summarize, AI changes perceptions of banking operations by automating most routine processes, improving risk management systems, detecting fraud, and providing personalized services. Future trends in banking will ride for more miles with changing AI technology.

2.1.4 Synergy of IoT, AI, and Blockchain in the Banking Sector

This transforms the banking ecosystem through the novel combination of the Internet of Things (IoT), Artificial Intelligence (AI), and blockchain technologies. Within their strengths, they enhance customer productivity, security experience, and much more.

1. **Enhanced Risk Management and Fraud Detection**

Indeed, combining the IoT, AI, and blockchain results in well-solid ground solutions regarding risk management when improving the detection of banking fraud. This is because IoT devices are said to generate real-time data from sources, either transactions or customer behavior; AI will then analyze such data and identify patterns that detect anomalies in fraudulent activity. For example, if an ATM detects unusual card usage in some odd place, AI algorithms might cross-check that with the historical data to assess the fraud risk. Blockchain provides an immutable record of all transactions in a secure manner. Its data utilization ensures information utilization for fraud detection without any scope for tampering. This integration has heavily enhanced the banks' capability to prevent and respond to fraudulent activities (PwC 2019).

2. **Streamlined Compliance and Regulatory Reporting**

Very sensitive to monetary policies, banking needs to simplify the complicated process involved. IoT, AI, and blockchain synergy make this happen through real-time tracking and recording of transaction data and compliance-related information on IoT devices. AI system analysis ensures that all activities are brought to a perfect check for regulatory compliance and is a source of insights for the audit. As it comprises transparent, immutable ledgers, blockchain technology supports security. That allows it to simplify the regulatory reporting process while initiating fewer errors and making compliance more precise and punctual than other alternatives (IBM Research 2021).

3. **Personalized Banking Services**

Integrating AI-driven insights into the IoT data enables banks to create highly personal experiences. IoT devices gather intricate customer preferences and behavior data using mobile applications and smartwatches. Based on this data, AI analyzes it to give particular financial advice and offers related to the product or service. For instance, data collected from customers' spending habits could indicate customized savings plans or investment options. Blockchain enhances personalization through the secure storage and management of customer data while ensuring its confidentiality and integrity. This synergy allows banks to give customers a more personalized and interactive experience (McKinsey Company 2020).

4. **Efficient Payment Systems**

Therefore, integrating IoT, AI, and blockchain into payment systems makes them speedier, safer, and more efficient. IoT enables contactless and automatic payment, while AI is applied to optimize the payment process through analyzing transactional data, fraud detection, and efficiency. Blockchain provides a safe and transparent ledger in every transaction made to eradicate error possibilities and fraud. For example, while transactions can be processed automatically in an Internet of things-based payment mechanism, AI monitors and optimizes them in real time; blockchain ensures only the same set of records are accurate and secured (Zhang et al. 2016; Zhao et al. 2018; Zohar 2015; Zcash 2021; Winding Tree 2018; World Bank 2020; Yearn.Finance 2021).

5. **Optimized Asset and Resource Management**

IoT enables real-time monitoring of the bank's assets. IoT devices can monitor ATMs, branch infrastructure, and security systems, providing insights on required asset maintenance, resource allocation optimization, and operational efficiency improvement. With this, blockchain can ensure the safe recording of transactions or ownership change through some blockchain mechanism. For example, IoT sensors may realize that the ATM has little or low cash or needs servicing; AI may predict when to come and to service it, while blockchain records all secure transactions involving the asset. The integration improves asset management and reduces operations costs (Deloitte 2020).

6. **Improved Customer Engagement and Loyalty**

Therefore, this synergy of IoT, AI, and blockchain provides innovative and secure banking experiences that boost and enhance customer engagement and loyalty. First, IoT devices such as intelligent ATMs and mobile banking ensure easy, seamless interactions. AI provides personal recommendations and support to customers, and blockchain gives security and transparency to all customer interactions and transactions. For example, a customer who uses a smart device to contact his bank is offered, based on AI's analysis of his transaction data. All communications are, of course, safely stored in a blockchain ledger. Such symbiosis creates trust and loyalty from customers (Capgemini 2021a, b, c).

Altogether, the interaction of IoT, AI, and blockchain lays down many measures to develop innovations in banking because they, in a real sense, improve risk management, compliance ease, personalization of service, optimization of payment systems, and asset management improvement. Indeed, it is expanding a new standard of efficiency and security in the banking sector.

2.2 Banking Applications of Blockchain

Blockchain has massive growth potential in most areas of the banking enterprise. In its decentralized, secure, and transparent form, blockchain promises to deliver a much more efficient, cost-effective, and safe banking method. The following are a few critical applications of blockchain technology in banking, as shown in Fig. 2.2.

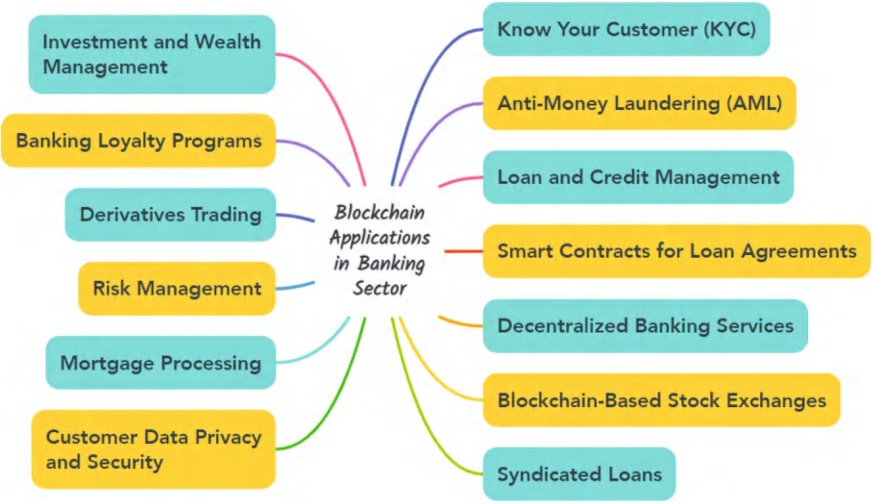

Blockchain Applications in Banking Sector
Investment and Wealth Management
Banking Loyalty Programs
Derivatives Trading
Risk Management
Mortgage Processing
Customer Data Privacy and Security
Know Your Customer (KYC)
Anti-Money Laundering (AML)
Loan and Credit Management
Smart Contracts for Loan Agreements
Decentralized Banking Services
Blockchain-Based Stock Exchanges
Syndicated Loans

Fig. 2.2 Blockchain applications in banking [compiled by researcher]

2.2.1 Know Your Customer (KYC)

Know Your Customer (KYC) is a prominent banking and finance process that makes verifying customers' identities possible. It is about preventing fraud, money laundering, and many more illicit activities. Traditional KYC processes are cumbersome, slow, and error-prone because of multiple intermediaries and their manual procedures. Blockchain technology is one of the new inventions with innovative solutions for enhancing and streamlining the process of KYC.

Overview of KYC Challenges

1. **Complex and Time-Consuming Procedures**:
   - **Manual Verification**: Most traditional KYC processes suffer from time-consuming and error-prone manual verification of documents (KPMG 2019).
   - **Multiple Submissions**: Customers are required to submit their KYC documents to several institutions. This means that several efforts are not very effective (PwC 2020).
2. **Lack of Data Privacy and Security**:
   - **Centralized Storage**: A centralized database where the KYC details are stored is prone to theft and unauthorized access (Gartner 2019).
   - **Data Protection Issues**: The processing and disclosing of such sensitive personal information would raise privacy and compliance concerns (GDPR 2018).

3. **High Costs**:
    - **Operational Costs**: Being utterly process-oriented and non-streamlined, the conventional procedure for KYC is costly for financial institutes (KPMG 2019).

Blockchain Solutions for KYC

1. **Decentralized Identity Verification**

Overview:

- **Blockchain Solution**: Blockchain will allow the construction of a decentralized electronic identity, where each individual owns and controls the record of identification information safely on a blockchain ledger (Catalini and Gans 2016).
- **Benefits**: Decentralized Identities remove verification, usually through multiple verifications, as it provides a single tamper-proof record sharable cross-institutional lines with consent from the users (Sovrin Foundation 2021).

Example:

- **SelfKey**: A blockchain-based digital identity system allows users to safely store and keep their identity data and share it with multiple service providers when necessary (SelfKey 2021).

2. **Improved Data Security and Privacy**

Overview:

- **Blockchain Solution**: The cryptographically congenial nature of blockchain and the immutable ledger ensures that no alteration can be made to KYC data without detection. Thus, personal data is encrypted, decentralized, better protected, and secure (Christidis and Devetsikiotis 2016).
- **Benefits**: Enhanced security and privacy would reduce some risks from data breaches and unauthorized access (Narayanan et al. 2016).

Example:

- **ID2020**: ID2020 is an initiative that uses the blockchain to help individuals obtain secure digital identities with privacy, zeroing in on protecting personal data and maintaining the user's privacy (ID2020 2018).

3. **Streamlined Verification Processes**

Overview:

- **Blockchain Solution**: Blockchain can automate and streamline KYC processes using smart contracts. Smart contracts are coded contracts whereby terms of the agreement are directly written into codes, which makes automatic verification and compliance checks possible (Christidis and Devetsikiotis 2016).
- **Benefits**: Automation minimizes manual intervention, will be much faster during verification, and reduces operational costs (PwC 2020).

Example:

- **RippleNet**: RippleNet applies blockchain to help simplify its processes, such as KYC with the bank and financial partners, to expedite customer identity verification processes (Ripple 2021).

4. **Enhanced Data Accuracy and Integrity**

Overview:

- **Blockchain Solution**: Because the data on the blockchain cannot be changed without leaving traces, the moment the KYC data is placed there, it cannot be modified, thus enhancing the accuracy and integrity of the data (Narayanan et al. 2016).
- **Benefits**: Accurate information reduces inconsistencies and errors in KYC documents, which is more convenient for trust and reliability (Christidis and Devetsikiotis 2016).

Example:

- **The Bank of England**: The Bank of England proposed blockchain solutions to ensure the exactness and trustworthiness of KYC data. It implemented the system to ensure a safe and secure KYC infrastructure (Bank of England 2020).

5. **Regulatory Compliance**

Overview:

- **Blockchain Solution**: Blockchain can also attain regulatory compliance since all the KYC activities will be recorded transparently and non-alterable. All these would facilitate meeting regulatory requirements and allow easier auditability (PwC 2020).
- **Benefits**: The very transparent ledger of the blockchain makes it easier to prove compliance and enhances the openness of the KYC procedure (Gartner 2019).

Example:

- **Kiva Protocol**: The Kiva Protocol uses blockchain to improve regulatory compliance by creating an open, auditable record of KYC processes and transactions (Kiva 2021).

Challenges and Considerations

1. **Integration with Existing Systems**

    - **Compatibility**: Merging blockchain-based KYC solutions with traditional banking systems and regulatory frames might take a long time and should be strategically planned (PwC 2020).
    - **Data Migration**: Moving existing KYC data to blockchain requires guaranteeing secure and efficient data transfer processes (Christidis and Devetsikiotis 2016).

2. **Regulatory and Legal Issues**

   - **Compliance**: Blockchain-based KYC solutions should obey financial regulations and data protection laws (GDPR 2018).
   - **Legal Framework**: A legal framework must be created that ensures the well-being of users' rights and privacy while permitting blockchain-based applications in the processes of KYC (ID2020 2018).

3. **Scalability and Performance**

   - **Transaction Throughput**: Millions of KYC transactions are meant to be processed by the blockchains. To accommodate the humongous financial transactions, it therefore calls for an assurance of scalability (Narayanan et al. 2016).
   - **Latency**: KYC Data processing and verification takes very minimum latency to support a real-time responsive service (Christidis and Devetsikiotis 2016).

2.2.2 Anti-money Laundering (AML)

It builds anti-money laundering (AML) and better knows your customer (KYC) processes regarding safety and transparency in storing and verifying identities and transactions between customers and organizations through blockchain technology. Blockchain can help make a tamper-proof record of KYC data for financial institutions to conduct due diligence more effectively and, at the same time, maintain regulatory compliance. Also, more effective monitoring and subsequent detection of suspicious activities by the system blockchain.

2.2.3 Loan and Credit Management

The loan and credit management of the bank and financial industry is associated with loan and credit facilities. This mainly encompasses issuing, serving, and managing loans and credit facilities. Generally, traditional loan and credit management systems are characterized by inefficiency, cost, and lack of transparency. Blockchain technology, therefore, might present an innovation towards solving such inefficiencies, coupled with security and transparency in loan and credit management.

Overview of Traditional Loan and Credit Management Challenges

1. **Inefficiencies in Processing**

   - **Manual Procedures**: Traditional loan processing involves lengthy manual procedures such as documentation, verification, and approval, which are prone to delays and mistakes (McKinsey Company 2020).

- **Intermediaries**: The rising number of multiple layers of intermediaries in loan-making and loan servicing adds complexity and processing time (World Bank 2020).

2. **High Costs**

   - **Operational Costs**: Servicing and loan management are very high, mainly due to administrative and compliance cost elements (Deloitte 2021).
   - **Fraud Risk**: The traditional systems lack fraud risk, which results in losses in the financial books and increased bank expenditures (Gartner 2019).

3. **Lack of Transparency and Data Integrity**

   - **Data Management**: There is a massive failure in the traditional mechanism to accurately update and maintain credit history records and loan agreements (PwC 2020).
   - **Transparency Issues**: The continued opaque loan and credit management process results in some disputes and issues related to regulatory non-compliance (KPMG 2019).

Blockchain Solutions for Loan and Credit Management

1. **Automated Loan Processing with Smart Contracts**

Overview:

- **Blockchain Solution**: These are self-executing contracts where the terms of the agreement are written directly into code. This process automatically executes loan agreements; most multiple intermediaries and manual processing also make redundant (Christidis and Devetsikiotis 2016).
- **Benefits**: Automation through smart contracts accelerates loan processing, minimizes errors, and reduces operations costs (McKinsey Company 2020).

Example:

- **Spring Labs**: Spring Labs utilizes blockchain and smart contracts to automate loan processing and credit risk evaluation, which allows it to be efficient and take less time to process (Labs 2021).

2. **Enhanced Transparency and Data Integrity**

Overview:

- **Blockchain Solution**: Blockchain offers the solution through an immutable, transparent ledger of all transactions—a method to document loan agreements and credit history without any amendments or changes (Narayanan et al. 2016).
- **Benefits**: The integrity and clarity of the data have enhanced, and disputes and regulatory compliance have decreased (PwC 2020).

Example:

- **Credit Bank of Moscow**: Credit Bank of Moscow uses blockchain solutions to manage loans to increase transparency and integrity within such processes by providing real-time access to accurate loan records (Credit Bank of Moscow 2020).

3. **Decentralized Credit Scoring**

Overview:

- **Blockchain Solution**: Blockchain enables decentralized credit scoring systems where credit history and scores are accessed securely and transparently. Reliance on traditional credit bureaus is decreased, but access to credit increases (Catalini and Gans 2016).
- **Benefits**: Decentralized credit scoring minimizes the possibility of errors and fraud and provides greater accuracy in representing the score for creditworthiness (Gartner 2019).

Example:

- **Bloom Credit**: Bloom Credit employs blockchain technology to provide customers with decentralized credit scoring. This allows clients' credit data to be managed safely and shared (Credit 2021).

4. **Streamlined Loan Origination and Servicing**

Overview:

- **Blockchain Solution**: Blockchain can simplify loan origination and servicing by implying a shared common ledger among interested stakeholders within the loan cycle. That means the cases of multiple entries and reconciliations will be fewer well (Deloitte 2021).
- **Benefits**: It simplifies the process that expedites loan origination and reduces administrative costs while improving the customer experience (McKinsey Company 2020).

Example:

- **Figure Technologies**: Figure Technologies has used blockchain technology to make loan origination and servicing easier, more efficient, and faster (Figure Technologies 2021).

5. **Improved Risk Management**

Overview:

- **Blockchain Solution**: It would ensure real-time immutability and accuracy of loan and credit management information, leading to better risk assessment and decision-making (World Bank 2020).

- **Benefits**: Stronger and more resilient lending operations reduce the number of defaults and losses with improved risk handling (PwC 2020).

Example:

- **The Bank of New York Mellon**: The Bank of New York Mellon has also explored blockchain solutions to improve risk management by displaying real-time and transparent data concerning loan portfolios and credit exposures (Bank of New York Mellon 2020).

Challenges and Considerations

1. **Integration with Legacy Systems**
   - **Compatibility**: Blockchain systems are not easy to integrate with traditional loan and credit management systems; hence, changes are pertinent to existing systems (PwC 2020).
   - **Data Migration**: Existing loan and credit data should also be migrated onto the blockchain platforms securely and efficiently to support continuation and accuracy (Christidis and Devetsikiotis 2016).
2. **Regulatory Compliance**
   - **Compliance**: Ensuring blockchain-based loan and credit management solutions adhere to statutory requirements and financial regulations is of tremendous importance (GDPR 2018).
   - **Legal Framework**: There is a need to evolve legal frameworks that allow blockchain in lending but protect consumer rights and keep all their data private (KPMG 2019).
3. **Scalability and Performance**
   - **Transaction Throughput**: Blockchain networks should be able to process large scales of loan transactions efficiently. Scaling up to meet the requirements of large-scale lending operations is quite essential (Narayanan et al. 2016).
   - **Latency**: Low latency for loan processing and servicing was crucial in ensuring timely responsive services (Christidis and Devetsikiotis 2016).

2.2.4 Smart Contracts for Loan Agreements

Smart contracts can, therefore, be described as self-executing contracts, whereby the contract is written directly into code and applies automatically upon the occurrence of certain predefined conditions. Smart contracts ensure various benefits regarding the management of loan agreements. This leads to the underpinnings of blockchain technology that provide better efficiency, transparency, and security for loan agreements within the financial sector.

Overview of Traditional Loan Agreements

1. **Manual Processing**
   - **Documentation**: Traditional lending arrangements require copious paperwork that is handled manually. Such activity tends to be very time-consuming and error-prone (McKinsey Company 2020).
   - **Approval Delays**: Loans processing and disbursals often involve several stages and intermediaries and, as such, tend to be tardy (Deloitte 2021).
2. **Lack of Transparency**
   - **Information Asymmetry**: The systems in place are not transparent. Hence, there is an inconsistency in monitoring the status of loan agreements in terms of compliance (PwC 2020).
   - **Dispute Resolution**: Even in disputes over the loan terms or its execution, an accessible, fixed record would seem to be easily avoided (Gartner 2019).
3. **High Costs**
   - **Administrative Costs**: Handled and administered loan agreements have brought severe administrative and operating costs (KPMG 2019).
   - **Fraud Risk**: Manual handling of loan agreements increases fraud and error risks (Narayanan et al. 2016).

Blockchain and Smart Contracts for Loan Agreements

1. **Automated Execution of Loan Terms**

Overview:

- **Blockchain Solution**: Smart contracts automatically automate loan agreement functions when preset conditions are met. Sometimes, predefined conditions have been reached, yet smart contracts automatically execute disbursements, payment schedules, interest calculations, and many others (Christidis and Devetsikiotis 2016).
- **Benefits**: Automation reduces human interventions, allows fast loan processing, and eradicates errors (McKinsey Company 2020).

Example:

- **Figure Technologies**: Figure Technologies allows intelligent contracts to execute loan origination and servicing automatically. This ensures faster and more accurate processing of loan agreements (Figure Technologies 2021).

2. **Enhanced Transparency and Auditability**

Overview:

- **Blockchain Solution**: Here, the smart contracts get executed based on the blockchain, thus providing transparent and tamper-proof ledgers for every transaction. It ensures that all parties are at the same information level in verifying the execution of the terms of a contract (Narayanan et al. 2016).

- **Benefits**: Better transparency and auditability reduce disputes and compliance and help garner trust among parties (PwC 2020).

Example:

- **Propy**: Propy uses blockchain-based smart contracts to run property transactions, which means it is very transparent and has less chance of a dispute, as every transaction is clear and immutable (Propy 2021).

3. **Improved Security**

Overview:

- **Blockchain Solution**: The characteristics of blockchain as a decentralized platform combined with intelligent contracts mean protection for loan contracts, which are encrypted and randomly located across several nodes in the network to discourage and prevent fraud and tampering (Christidis and Devetsikiotis 2016).
- **Benefits**: Enhanced safety feature safeguards information about the loan agreement, safeguarding against theft and fraud by unauthorized access (Gartner 2019).

Example:

- **SmartContract**: SmartContract uses blockchain technology to set up tamper-proof, secure smart contracts for various financial agreements, like loans, providing better security (SmartContract 2021).

4. **Efficient Management and Administration**

Overview:

- **Blockchain Solution**: With this feature, smart contracts can also ease further the process of loan agreement administration and management by setting dates for payment and interest application (Deloitte 2021).
- **Benefits**: Efficient management reduces administrative overhead and operation costs, ensuring efficient loan management (McKinsey Company 2020).

Example:

- **Centrifuge**: Centrifuge utilizes blockchain-based smart contracts in order to manage and automate invoice and loan administration, thus saving time and cost (Centrifuge 2021).

5. **Risk Mitigation**

Overview:

- **Blockchain Solution**: Smart contracts could contain multiple risk mitigation features, such as the automated management of defaults and penalty enforcement according to predefined conditions (Christidis and Devetsikiotis 2016).

- **Benefits**: Automation of risk management decreases the likelihood of defaults and ensures legal satisfaction of all contractual obligations (Narayanan et al. 2016).

Example:

- **OpenLaw**: OpenLaw introduced smart contracts to automatically manage the risks of loan agreement, penalty enforcement and managing defaults (OpenLaw 2021).

Challenges and Considerations

1. **Legal and Regulatory Compliance**
    - **Legality**: The legality status and effect of the enforcement of smart contracts differs from jurisdiction to jurisdiction. Therefore, observance of legal formalities and the applicable rules is also important (PwC 2020).
    - **Regulatory Framework**: A regulatory framework needs to be developed that supports the use of smart contracts in loan agreements while protecting consumer rights (KPMG 2019).
2. **Integration with Existing Systems**
    - **Compatibility**: Integration of smart contracts into the current loan management systems and financial infrastructure can be problematic and may demand drastic changes in the existing system (Deloitte 2021).
    - **Data Migration**: Migrate existing loan contracts into blockchain-based systems securely and efficiently (Christidis and Devetsikiotis 2016).
3. **Scalability and Performance**
    - **Transaction Throughput**: To make a blockchain scalable, it is important that it supports the processing of numerous loans at one time (Narayanan et al. 2016).
    - **Latency**: Execution of smart contract should be with lesser latency, and processing loan agreements should not be delayed (Christidis and Devetsikiotis 2016).

2.2.5 Decentralized Banking Services

Decentralized banking services, by leveraging blockchain technology, can access a financial system that provides functions almost like those of traditional banking but in a decentralized manner. It thus shows a minimum usage of central authorities and also the usage of intermediaries in nearly more accessible, transparent, and efficient financial services. DeFi colloquially referred to is a decentralized banking comprehensive array of services such as lending and borrowing, as well as asset management related to blockchain technology as well as smart contracts.

Overview of Traditional Banking Services

1. **Centralized Control**

   - **Intermediaries**: Bank Classical systems are based on intermediaries and central authority, i.e., banks, clearinghouses, and payment processors. Intermediaries may create inefficiencies and costs (McKinsey Company 2020).
   - **Limited Access**: In brief, proximity, regulatory restrictions, and other financial restraints might limit services up for grabs at banking (World Bank 2020).

2. **Cost and Complexity**

   - **High Fees**: Traditional banking services come with sky-high fees due to transactions, account maintenance, and other services (Deloitte 2021).
   - **Complex Processes**: Bank procedures are long and cumbersome with multiple steps and paper works, hence unnecessary delays and inefficiencies in banking (PwC 2020).

3. **Lack of Transparency**

   - **Opaque Operations**: Banking operations may be opaque as these entail minimal transparency of procedures and charges of transactions (KPMG 2019).
   - **Slow Transactions**: Transactions, particularly cross-border transactions, are slow and expensive due to various levels of mediaries (Gartner 2019).

Blockchain and Decentralized Banking Services

1. **Peer-To-Peer Lending and Borrowing**

Overview:

- **Blockchain Solution**: There is direct peer-to-peer lending and borrowing in decentralized platforms without traditional financial intermediaries. This includes situations where smart contracts will execute automatically for terms depending on predefined conditions (Christidis and Devetsikiotis 2016).
- **Benefits**: Include lower expenses, increased availability of credit and quicker settlement of transactions (McKinsey Company 2020).

Example:

- **Aave**: Aave is a noncustodial protocol; it allows direct lending and borrowing of assets among users. Smart contracts governing transactions are involved in this process (Aave 2021).

2. **Decentralized Exchanges (DEXs)**

Overview:

- **Blockchain Solution**: Decentralized exchanges enable cryptocurrencies and other digital assets to be traded peer-to-peer directly between users sans a central authority. These systems rely on smart contracts to make and secure transactions (Narayanan et al. 2016).

- **Benefits**: Increased transparency, reduced counterparty risk, and lower fees are notable benefits (PwC 2020).

Example:

- **Uniswap**: This is a decentralized exchange where users will directly trade Ethereum-based tokens with each other using automated market-making algorithms (Uniswap 2021).

3. **Decentralized Asset Management**

Overview:

- **Blockchain Solution**: Decentralized asset management platforms will provide investment services and portfolio management through blockchain. Smart contracts will manage the assets and execute trades based on criteria defined by users (Christidis and Devetsikiotis 2016).
- **Benefits**: It provides easier access to investment, lower fees, and greater transparency (McKinsey Company 2020).

Example:

- **Yearn.Finance**: Yearn.Finance provided decentralized asset management services. This protocol optimizes yield farming strategy and manages the portfolio with smart contracts (Yearn.Finance 2021).

4. **Stablecoins and Digital Currencies**

Overview:

- **Blockchain Solution**: Stablecoins are digital currencies pegged to a stable asset, such as a fiat currency, to mitigate volatility. These are often used within decentralized banking platforms for the purpose of transactions and value storage (Narayanan et al. 2016).
- **Benefits**: Safety, value, and usability in decentralized finance applications (Gartner 2019).

Example:

- **USDC**: USD Coin (USDC) is a stable coin pegged to the value of the US dollar. It’s very common in decentralized finance-used for facilitating transactions and as collateral (Centre Consortium 2021).

5. **Decentralized Insurance**

Overview:

- **Blockchain Solution**: Blockchain along with smart contracts is used in the decentralized insurance platforms, which provide the service independent of the intermediaries. Claims are automatically passed and payments initiated based on the predefined conditions (Christidis and Devetsikiotis 2016).
- **Benefits**: Cost savings, more transparency and faster settlement of claims (PwC 2020).

Example:

- **Nexus Mutual**: Nexus Mutual offers peer-to-peer, decentralized insurance. Through a blockchain-based platform, users pool funds to contribute towards covering one's risk (Nexus Mutual 2021).

Challenges and Considerations

1. **Regulatory Uncertainty**
    - **Compliance**: Regulatory environment for Decentralized banking services is still in their relative infancy. Means ensuring compliance with existing banking and financial regulations and adaptation to new ones (KPMG 2019).
    - **Legal Framework**: Adequate legal structure in support of decentralized banks that will help prevent consumer exploitation and ensure financial stability is required (World Bank 2020).
2. **Security and Risk Management**
    - **Smart Contract Vulnerabilities**: With smart contracts carrying an entry point for bugs and exploitation, security is improved in blockchain. The security measures also rely on good robust measures and regular audits (Narayanan et al. 2016).
    - **Market Risks**: Volatility in digital assets and manipulation may be big risks to decentralized financial services (McKinsey Company 2020).
3. **Scalability and Performance**
    - **Transaction Speed**: Scaling decentralized platforms to scale for thousands of large transactions per second is a problem. Solutions in this space include layer 2 scaling and the development of new consensus algorithms (Deloitte 2021).
    - **Network Congestion**: This involves the need to handle network congestion and decentralized service smooth operation, especially for the user experience (Christidis and Devetsikiotis 2016).

2.2.6 *Blockchain-Based Stock Exchanges*

Blockchain-based stock exchanges are essentially the next step in the evolution of financial markets. These are decentralized platforms that would take over old forms of a stock exchange; through Blockchain technology, indeed use would enhance the efficiency, transparency, and security of transactions around trading. Blockchain is what makes decentralization possible and for immutable ledgers, so it does enable realizing stock exchange designs with reduced dependency on central authorities or middlemen.

Overview of Traditional Stock Exchanges

1. **Centralized Control**

   - **Intermediaries**: It is interfaced with the traditional stock exchange through such intermediaries as clearinghouses, brokers, and custodians in order to facilitate and settle transactions. Centralization may cause inefficiencies and delays (McKinsey Company 2020).
   - **Regulatory Compliance**: Legacy exchanges operate in pretty heavy-duty regulatory regimes, which often results in slower innovations and higher compliance costs (Deloitte 2021).

2. **Settlement Times and Costs**

   - **T + 2 Settlement**: Most archaic stock exchanges follow the T + 2 settlement cycle, referring to two business days after the trade date; this delays the actual final transfer of ownership and has a number of intermediaries (PwC 2020).
   - **High Fees**: Multiple parties are involved, and this marks the occurrence of transaction fees, brokerage fees, and other administrative expenses at a high cost (Gartner 2019).

3. **Transparency and Security**

   - **Opaque Processes**: Opaque processes of traditional stock exchanges tend to lack transparency in trading processes and data (KPMG 2019).
   - **Fraud Risk**: The traditional type of exchange is weak to fraud and security breaches because of its central characteristic (Narayanan et al. 2016).

Blockchain and Blockchain-Based Stock Exchanges

1. **Decentralized Trading Platforms**

Overview:

- **Blockchain Solution**: Blockchain-based stock exchanges operate from decentralized mediums where trades are executed and settled using smart contracts and blockchain technology. This removes the intermediaries and authority centralities of old (Christidis and Devetsikiotis 2016).
- **Benefits**: Important advantages include lower cost of transactions, faster settlement time, and greater transparency (McKinsey Company 2020).

Example:

- **tZERO**: tZERO is an online blockchain-related site offering its users the opportunity for the exchange of digital securities and tokenized assets. It would make people create a highly efficient yet transparent environment that compares with traditional exchanges (tZERO 2021).

2. **Tokenization of Securities**

Overview:

- **Blockchain Solution**: Blockchain enables traditional security products like shares and bonds to be tokenized. Tokenization is the process whereby such assets are converted into electronic tokens, traded on blockchain platforms (Narayanan et al. 2016).
- **Benefits**: Tokenization may bring in higher liquidity, cheaper transaction costs, and fractional ownership (PwC 2020).

Example:

- **Polymath**: Polymath is the world's first issuing and managing platform for security tokens, which allows tokenizing traditional securities (Polymath 2021).

3. **Enhanced Transparency and Security**

Overview:

- **Blockchain Solution**: For every and each transaction, blockchain provides an immutable, public ledger that improves both transparency and security with regard to the trading activity. Smart contracts enable automatic execution and settlement of trades, whose risk of fraud is reduced (Christidis and Devetsikiotis 2016).
- **Benefits**: Enhanced clarity and security diminish market manipulation and allow for equitable trade practices in the market (McKinsey Company 2020).

Example:

- **The Open Platform**: The Open Platform bases its advantages on blockchain to provide more transparent and secure trading, thus adopting a decentralized solution for the stock exchanges (The Open Platform 2021).

4. **Real-Time Settlement**

Overview:

- **Blockchain Solution**: Blockchain-based exchanges enable immediate settlement of trades, thus eliminating the time gap between an executed trade and its settlement as is against traditional T + 2 systems (Gartner 2019).
- **Benefits**: Faster settlement times reduce a counterparty risk and increase market efficiency (Deloitte 2021).

Example:

- **Nasdaq Linq**: Nasdaq Linq is a blockchain technology company that enables the instant settlement of over private securities through optimal efficiency in trading and settlement (The Open Platform 2021).

5. **Global Accessibility**

Overview:

- **Blockchain Solution**: Block-chain-based stock exchanges can provide worldwide reach, including investor's capability from various regions to trade without using local intermediaries (Christidis and Devetsikiotis 2016).
- **Benefits**: Openness and access to market will increase an individual's accessibility to the financial markets (McKinsey Company 2020).

Example:

- **Bitfinex**: Bitfinex (2021) is a global trading platform using blockchain; it provides trade and access to a super high variety of digital assets and securities (Kiva 2021).

Challenges and Considerations

1. **Regulatory Compliance**
    - **Legal Framework**: Blockchain-based stock exchanges will face complex regulatory environments through compliance with extant financial regulations and securities laws (KPMG 2019).
    - **Regulatory Approval**: It is very hard to get regulatory approvals for blockchain-based platforms as they pose several security, transparency, and integrity issues of the market (Deloitte 2021).
2. **Technological Challenges**
    - **Scalability**: The ability of the blockchain platforms to effectively handle voluminous trade and large-scale transactions is extremely critical (Narayanan et al. 2016).
    - **Integration**: The integration of blockchain-based systems with the existing financial infrastructure and being compatible with the traditional system poses a challenge (PwC 2020).
3. **Market Adoption**
    - **Industry Resistance**: Traditional financial institutions and market participants are resistant to change because of inertia as well as loss of security and reliability as apprehended in the traditional way (Gartner 2019).
    - **Education and Training**: The participants in the market must be educated on the benefits and functionality associated with blockchain-based exchanges for mass adoption (McKinsey Company 2020).

2.2.7 Customer Data Privacy and Security

Customer data privacy and security are critical considerations in blockchain-based banking systems. It remains particularly important because it arises when financial services begin to adopt the use of the blockchain technology. In fact, with features like immutability and decentralization in the blockchain, it presents potential but poses a challenge in the safeguarding of data privacy and security.

Overview of Traditional Banking Data Privacy and Security

1. **Centralized Data Storage**

Centralized Systems:

- **Intermediaries**: In the traditional banking system, customer data is typically maintained through centralized databases operated by the financial institutions. Centralization involves single points of failure and makes them especially attractive targets (KPMG 2019).
- **Regulatory Compliance**: Banks must comply with regulations such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act) to protect customer data (PwC 2020).

2. **Risk of Data Breaches**

Vulnerabilities:

- **Cyberattacks**: Centralized databases are vulnerable to cyberattacks, data breaches, and hacking cases. A cyberattacker can easily steal sensitive details of customers and cause financial and reputational loss (McKinsey Company 2020).
- **Internal Threats**: Also real are the internal threats-those where employees improperly use access to customer data (Deloitte 2021).

3. **Data Handling and Storage**

Challenges:

- **Data Handling**: Handling large volumes of customer data with integrity, ensuring confidentiality is quite challenging. Such traditional systems usually involve complex procedures for obtaining and exercising controls over data access (Gartner 2019).
- **Data Storage**: The sensitive data is stored safely and protected from unauthorized access, and this becomes an ongoing challenge (Narayanan et al. 2016).

Blockchain and Customer Data Privacy and Security

1. **Immutable Ledger**

Overview:

- **Blockchain Solution**: Once data is entered into the blockchain, it cannot be changed or altered. Obviously, this boosts data integrity, thus greatly reducing the opportunities for manipulation (Christidis and Devetsikiotis 2016).

- **Benefits**: The opportunities for maintaining integrity and auditing increase since all modifications regarding the data are always recorded as new transactions (McKinsey Company 2020).

Example:

- **Chainalysis**: Chainalysis is bringing blockchain analytics to enable data integrity and traceability in cryptocurrency transactions, thus ensuring both security and transparency (Thomas 2009).

2. **Decentralization**

Overview:

- **Blockchain Solution**: With distributed storage of customer data in a decentralized network, it reduces reliance on potential single points of failure and limits the potential damage from eventual breaches (Christidis and Devetsikiotis 2016).
- **Benefits**: The advantage of the distributed control improved security, and diminished large-scale likelihood of data leaks (PwC 2020).

Example:

- **Filecoin**: Filecoin, as such, is a decentralized storage network whose functionalities utilize blockchain technology to secure and manage data storage in distributed networks (Filecoin 2021).

3. **Cryptographic Protection**

Overview:

- **Blockchain Solution**: Blockchain employs some advanced cryptographic techniques to secure data, such as encryption and hashing. These methods ensure the customer data is protected against unauthorized access and privacy (Narayanan et al. 2016).
- **Benefits**: Information is encrypted and hashed so that the unwanted third parties cannot achieve the file or any information in it (McKinsey Company 2020).

Example:

- **Zcash**: Zcash stays with their privacy cryptocurrency through advanced crypto-techniques that hide the transaction data (Zcash 2021).

4. **Smart Contracts for Data Access Control**

Overview:

- **Blockchain Solution**: Smart contracts can automatically and enforce data access controls, where the access or modification of customer's information becomes accessible to only certain authorities (Christidis and Devetsikiotis 2016).
- **Benefits**: Automated and transparent control access arrangements eliminate unauthorized access to data (Deloitte 2021).

Example:

- **Hyperledger Fabric**: It supports smart contracts for enterprise blockchain applications, in order to manage access controls and data privacy (Hyperledger 2021).

5. **Data Anonymization and Privacy Preservation**

Overview:

- **Blockchain Solution**: Anonymize data through zero-knowledge proofs, yet simultaneously that transactions are verified. This would allow privacy, yet provide transparency (Narayanan et al. 2016).
- **Benefits**: More robust customer data privacy, hence, harder to verify the transaction without de-anonymizing data (PwC 2020).

Example:

- **zk-SNARKs**: zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) are used in privacy coins to enhance data protection and privacy (Zcash 2021).

Challenges and Considerations

1. **Data Privacy Regulations**
   - **Compliance**: With data privacy, blockchain system also adheres to the GDPR and CCPA compliance that requires data protection based on user consent (KPMG 2019).
   - **Regulatory Challenges**: Compliance with constantly changing global data privacy regulations is complex for blockchain-based systems (PwC 2020).
2. **Scalability and Performance**
   - **Scalability Issues**: Blockchain networks may have low performance in dealing with large data volumes, and this again affects performance and privacy (Gartner 2019).
   - **Performance Trade-offs**: In blockchain systems, the conflict between privacy and performance demands such critical balancing in cryptography techniques and data storage solutions (Christidis and Devetsikiotis 2016).
3. **User Education and Awareness**
   - **Awareness**: In the blockchain, educating clients about data privacy and security measures induces trust and proper usage (McKinsey Company 2020).
   - **Transparency**: Transparency towards clarification of the handling of data and other privacy protections helps build customer confidence (Deloitte 2021).

2.2.8 Mortgage Processing

Mortgage processing comes under the complex area of financial services that involves stages such as application, underwriting, approval, and servicing. It is definitely possible to introduce blockchain technology in mortgage processing to create higher efficiency, transparency, and security domains. The fact that the blockchain ledger is decentralized and immutable affords inventive ways of streamlining mortgage workflow and reducing overhead costs for administration.

Traditional Mortgage Processing

1. **Application and Documentation**

Current Practices:

- **Paper-Based Systems**: The traditional mortgage processing system requires a lot of paperwork and manual data entry. Borrowers have to provide many documents, which include income statements, credit reports, and proof of assets (Deloitte 2021).
- **Data Entry Errors**: Tendency of data entry errors and inefficiencies, hence processing delays are associated with manual processing (PwC 2020).

2. **Underwriting and Approval**

Current Practices:

- **Manual Verification**: Underwriting provides credit analysis, document verification, and risk assessment. A process that is mainly done manually, taking a number of checks (McKinsey Company 2020).
- **Processing Delays**: Underwriting would take ample time as so many verifications and approvals from various quarters need to be processed (Gartner 2019).

3. **Settlement and Servicing**

Current Practices:

- **Complex Transactions**: Settlement involving a mortgage is a triple party-of the lender, title company, and escrow agent. Complexity involved in this causes bottlenecks as well as expense (KPMG 2019).
- **Servicing Challenges**: The processes of servicing from mortgage, including paying and accounts managing, are normally followed manually and written down (Narayanan et al. 2016).

Blockchain Solutions for Mortgage Processing

1. **Digital Identity Verification**

Overview:

- **Blockchain Solution**: The blockchain will let digital identity authenticate through decentralized identity management systems that are profoundly safe. The blockchain-based digital identity can simplify the application process of borrowing for borrowers (Christidis and Devetsikiotis 2016).
- **Benefits**: It is faster and more secure identity verification, which reduces the overall documentary documentation level and improves the efficiency of the application process (McKinsey Company 2020).

Example:

- **SelfKey**: SelfKey is a blockchain-based identity verification platform that offers the first digital identity for safe financial services, including mortgage processing (SelfKey 2021).

2. **Smart Contracts for Automated Processing**

Overview:

- **Blockchain Solution**: Smart contracts may also automate approval and underwriting and payment among the processes involved in a mortgage cycle. They execute predefined rules and conditions automatically with minimal human involvement (Christidis and Devetsikiotis 2016).
- **Benefits**: More efficient and more accurate, as the processing time and cost are decreased because of automation (PwC 2020).

Example:

- **Uphold**: Maintain uses blockchain smart contracts to automate the flow of funds and agreement processes, including mortgages (Uphold 2021).

3. **Immutable Record Keeping**

Overview:

- **Blockchain Solution**: Blockchain provides an immutable ledger where all transactions including alterations to the documents are stored. The mortgage record is therefore safe, clear, and tamper-free (Narayanan et al. 2016).
- **Benefits**: The mortgage records will be very safer, transparent and full of integrity hence curbing frauds and disputes (Deloitte 2021).

Example:

- **Propy**: Propy uses blockchain in the real estate transaction management process, thereby providing safe and transparent record-keeping (Propy 2021).

4. **Streamlined Settlement Processes**

Overview:

- **Blockchain Solution**: Blockchain technology may be able to simplify the settlement process by real time, secure transactions and minimizing the intermediaries required (Christidis and Devetsikiotis 2016).
- **Benefits**: Faster and swifter settlements, lower transaction cost of transactions, and reliability (McKinsey Company 2020).

Example:

- **AlphaPoint**: AlphaPoint (2021) provides blockchain-based solutions in financial transactions and asset management, for example, mortgage settlements (Deloitte 2020).

5. **Fraud Prevention and Risk Management**

Overview:

- **Blockchain Solution**: Blockchain's transparency easily traces the perpetration of fraud, as every history of transaction and all changes made in the documents can be traced (Narayanan et al. 2016).
- **Benefits**: Less fraudulent activities and more risk management because of its real-time auditing and monitoring features (PwC 2020).

Example:

- **Everledger**: Everledger utilizes blockchain technology in tracing and authenticating the legitimacy of valuable assets that include real estate assets to prevent fraud (Everledger 2021).

Challenges and Considerations

1. **Regulatory Compliance**
   - **Legal Framework**: The blockchain-based mortgage system aligns with the current legal framework in place for data protection and financial regulatory needs (KPMG 2019).
   - **Regulatory Approval**: It is so tough to get the regulators' approval because such systems have to be aligned with such complex and varied requirements (Deloitte 2021).
2. **Integration with Legacy Systems**
   - **Compatibility**: Integrating blockchain-based solutions into the existing mortgage processing systems and infrastructure is relatively complex and capital-intensive (Gartner 2019).
   - **Data Migration**: Migration data integrity and security from traditional systems to blockchain platforms while remaining accurate is very important (McKinsey Company 2020).

3. **Adoption and Industry Acceptance**

    - **Resistance to Change**: Financial institutions and stakeholders resist the adoption process of the use of blockchain technology due to security, reliability, and disturbances in processes of previous existing strategies (PwC 2020).
    - **Education and Training**: Education and training approach the people in the industries about blockchain technology and all the benefits that can enhance its adoption (Christidis and Devetsikiotis 2016).

2.2.9 Syndicated Loans

Thus, **syndicated loans** mean a bank or some banks combine to provide large amounts of capital to the borrower, often corporations or governments. This group approach means lenders can pool resources and share the risk to offer substantial amounts of capital. Thus, in syndicated loan usage, blockchain technology will increase transparency, efficiency, and security in loan syndication.

Traditional Syndicated Loans Processing

1. **Loan Origination and Structuring**

Current Practices:

- **Manual Processes**: Typically, such syndicated loan negotiation and structuring involve several manual processes, including negotiation, documentations, and assessment of the risk (Deloitte 2021).
- **Complexity**: Much of this complexity entailed multiple lenders and borrowers, leading to a tendency towards inefficiency and delays (PwC 2020).

2. **Documentation and Compliance**

Current Practices:

- **Paper-Based Systems**: The traditional loan syndication is mostly always paper-based, with manual checks of compliance. It is sometime very time-consuming and error-prone too (McKinsey Company 2020).
- **Regulatory Compliance**: Mass documentation does bear a relation to the complexity, coupled with regulatory needs (Gartner 2019).

3. **Loan Administration and Servicing**

Current Practices:

- **Administrative Overhead**: There exists the cost of administering syndicated loans, which also involves tracking, settling payables, and communicating among parties (KPMG 2019).
- **Coordination Challenges**: This coordination is proving challenging between different lenders and the borrower, which will cause delay and inefficiency in processes (Narayanan et al. 2016).

Blockchain Solutions for Syndicated Loans

1. **Digital Loan Agreements**

Overview:

- **Blockchain Solution**: Blockchain technology facilitates an opportunity in which digital loan agreements may be created and handled through the use of smart contracts that'll automatically facilitate terms, conditions, and payments with minimal human interventive measure (Christidis and Devetsikiotis 2016).
- **Benefits**: Reduce administrative overheads with efficiency and accuracy due to automation of agreement execution and monitoring (PwC 2020).

Example:

- **Finastra**: Finastra uses blockchain based on smart contract loan syndication. It increases the efficiency and accuracy with regard to loans (Finastra 2021).

2. **Transparency and Auditability**

Overview:

- **Blockchain Solution**: Blockchain's immutable ledger provides transparent and tamper-proof records of all loans as well as any form of communication. Such a feature promotes transparency and auditing within the syndication process (Narayanan et al. 2016).
- **Benefits**: Trust among stakeholders increases while the chance for fraud or mistakes is minimized because the nature of the ledger is transparent (McKinsey Company 2020).

Example:

- **R3 Corda**: R3 Corda is a blockchain for syndicated loans that heightens the transparency of and auditability in financial transactions (CurioInvest 2021).

3. **Real-Time Updates and Notifications**

Overview:

- **Blockchain Solution**: Blockchain technology can automatically send in real-time information to all the stakeholders engaged in a syndicated loan. For example, smart contracts can alert parties of payments, adjustments, etc. (Christidis and Devetsikiotis 2016).
- **Benefits**: It enables faster and more efficient communication thereby reducing delays and updating all parties in real time (PwC 2020).

Example:

- **We.Trade**: We.Trade utilizes blockchain to embed real time updated and notice capabilities on trade finance and syndicated loans. This has improved efficiencies and coordination (Capgemini 2021a).

4. **Efficient Syndication and Distribution**

Overview:

- **Blockchain Solution**: Blockchain enables the potential of streamlining the syndication process by allowing for immediate loan portions disbursements for participants. The system therefore reduces intermediaries and also accelerates the flow (Christidis and Devetsikiotis 2016).
- **Benefits**: It reduces processing times and decreases administrative costs and also makes loans of distribution much more effective (McKinsey Company 2020).

Example:

- **Clearmatics**: Clearmatics offers a blockchain-based platform that automates loan syndication and distribution, aiming to make operations more efficient (Zohar 2015).

5. **Risk Management and Compliance**

Overview:

- **Blockchain Solution**: Blockchain's secure and transparent nature aids in managing risks and ensuring compliance with regulatory requirements. Real-time monitoring and auditing capabilities enhance risk management and regulatory adherence (Narayanan et al. 2016).
- **Benefits**: Real-time data accessibility by all teams strengthens risk management and supports compliance with regulatory standards (Deloitte 2021).

Example:

- **IBM Blockchain**: IBM blockchain represents an opportunity for risk management and compliance in syndicated loans, which can be engaged with newer and analytics-driven data (IBM Research 2021).

Challenges and Considerations

1. **Regulatory and Legal Framework**
   - **Compliance**: Blockchain-based syndicated loans have to be compliant with extant financial regulations and legal frameworks, which are, anyway, comprehensive and vary across jurisdictions (KPMG 2019).
   - **Regulatory Approval**: The blockchain-based syndication platforms may get regulatory approval most likely under more complicated legal and compliance terms (Deloitte 2021).

2. **Integration with Legacy Systems**
   - **Compatibility**: Blockchain-based solutions generally cannot compete with the existing financial systems and infrastructures. Investments can be made in building compatibility (Gartner 2019).

- **Data Migration**: The data of the traditional system has to be moved over to blockchain platforms securely and reliably (McKinsey Company 2020).

3. **Industry Adoption and Collaboration**

- **Resistance to Change**: Due to the security and reliability, banks are not willing to transform themselves into the blockchain technology because of breaking down of traditional processes (PwC 2020).
- **Collaboration**: Collaboration between the various stakeholders, including lenders, borrowers, and regulatory bodies, will contribute significantly to the smooth implementation process (Christidis and Devetsikiotis 2016).

2.2.10 Banking Loyalty Programs

Banking loyalty programs are targeting to award the consumer positively through patronizing the institution via continued patronage through rewards like points, cash back, and discounts, among many others. What they hope is that increase in customer engagement, retention, and eventually brand loyalty would result. The said program added with blockchain technology would be efficient, transparent, and secure.

Traditional Banking Loyalty Programs

1. **Program Design and Management**

Current Practices:

- **Manual Systems**: Such archaic loyalty programs are based on largely manual systems of accrual and rewards for customers; an exercise that demands far-fetched calculations and record-keeping (Deloitte 2021).
- **Limited Transparency**: The customer will see less into the balance of points, choice of reward, and program rules (PwC 2020).

2. **Reward Redemption**

Current Practices:

- **Complex Processes**: The redemption processes of credit are complex involving manual verification and fulfillment processes that time-consuming, thus prone to delay and customer dissatisfaction (McKinsey Company 2020).
- **Fragmented Systems**: Customer loyalty rewards are operated in fragmented systems which lead to a disloyal experience to customers (Gartner 2019).

3. **Fraud and Security**

Current Practices:

- **Fraud Risks**: These traditional systems are fraud and abuse vulnerable. This encompasses point theft or unauthorized access accounts (KPMG 2019).

- **Security Concerns**: The customer's details and their transaction cannot be secured properly in traditional loyalty programs (Narayanan et al. 2016).

Blockchain Solutions for Banking Loyalty Programs

1. **Transparent and Immutable Rewards Ledger**

Overview:

- **Blockchain Solution**: Blockchain provides an open and tamper-proof ledger to write down and trace up points and rewards accumulated in loyalty programs. This means that all transactions are secure and verifiable (Christidis and Devetsikiotis 2016).
- **Benefits**: Increased transparency and protection from a transaction record that is tamper-proof and reliable for loyalty points (PwC 2020).

Example:

- **LoyalCoin**: LoyalCoin utilizes the power of blockchain to create an open and secure system of loyalty points that enables customers to efficiently manage and redeem them (LoyalCoin 2021).

2. **Smart Contracts for Automated Reward Management**

Overview:

- **Blockchain Solution**: Smart contracts can automatically create rules and conditions that will govern management and redemption of rewards (Christidis and Devetsikiotis 2016).
- **Benefits**: Low administrative overhead, prompt processing of rewards, and high precision in handling loyalty points (McKinsey Company 2020).

Example:

- **Centrifuge**: Centrifuge uses blockchain-based smart contracts to automate different parts of loyalty programs, including point allocation and redemption (Centrifuge 2021).

3. **Integration with Multiple Loyalty Programs**

Overview:

- **Blockchain Solution**: Blockchain enables customers to link multiple loyalty programs on a single platform so that they are in a better position to manage their reward benefits (Christidis and Devetsikiotis 2016).
- **Benefits**: Easy handling of rewards, higher engagement of customers, and an assimilated experience of diverse programs (PwC 2020).

Example:

- **Token Rewards**: Token Rewards employs blockchain and connects different loyalty programs in a manner in which customers earn and redeem points across platforms (Finastra 2021).

4. **Enhanced Security and Fraud Prevention**

Overview:

- **Blockchain Solution**: Blockchain Solution Because of its secured and decentralized features, blockchain prevents fraud and unauthorized access to accounts in loyalty programs (Narayanan et al. 2016).
- **Benefits**: With a better point in thieving and fraud, security, and transactions are safe, and traceable (Deloitte 2021).

Example:

- **BitRewards**: BitRewards relies on the blockchain system to prevent fraud and secure payments and loyalty points (Deloitte 2021).

5. **Real-Time Tracking and Updates**

Overview:

- **Blockchain Solution**: Blockchain will track and update in real time the loyalty points and rewards so that customers can easily view their present balances and history of transactions in real time (Christidis and Devetsikiotis 2016).
- **Benefits**: It enhances customer experience through real-time updates and proper tracking of loyalty reward points (PwC 2020).

Example:

- **Blockpoint**: Blockpoint (2021) uses blockchain to track and update loyalty programs in real time, thus providing the latest information to clients (Bank of New York Mellon 2020).

Challenges and Considerations

1. **Regulatory Compliance**

    - **Legal Framework**: The existing legal framework, including data protection, financial transaction legislation, and customer protection, is applicable in blockchain-based loyalty programs (KPMG 2019).
    - **Regulatory Approval**: Obtaining regulatory compliance and gaining approval of blockchain-based solutions is quite a difficult challenge (Deloitte 2021).

2. **Integration with Existing Systems**

    - **Compatibility**: Implementation of blockchain solutions can require significant capitals and technical alignment with existing loyalty program's infrastructures (Gartner 2019).

- **Data Migration**: Migrating data from the legacy system to the blockchain-based platform in a secure and accurate way (McKinsey Company 2020).

3. **Adoption and Consumer Education**

- **Consumer Awareness**: Customers must be enlightened through the merits and usage of blockchain-based loyalty programs for full adoption to be achieved (PwC 2020).
- **Industry Acceptance**: Financial institutions and loyalty program firms have to face resistance to adopting new technology by the latter (Christidis and Devetsikiotis 2016).

2.2.10.1 Investment and Wealth Management

Investment and wealth management involve techniques and practices that produce growth in the financial assets of an individual or a firm over time. These may include portfolio management, investment strategy, risk management, among other elements of financial planning for future objectives. Blockchain technology is set to transform the field of investment and wealth management by enhancing transparency, efficiency, and security in most facets of the investment process.

Traditional Investment and Wealth Management

1. **Portfolio Management**

Current Practices:

- **Manual Tracking**: Most portfolios necessitate manual tracking of investments, performance analysis, and rebalancing (Deloitte 2021).
- **High Fees**: Traditional portfolio management services can have high management fees and commissions (PwC 2020).

2. **Transaction Processing**

Current Practices:

- **Intermediaries**: Transactions are typically processed through multiple intermediaries, including brokers and clearinghouses, which can introduce delays and increase costs (McKinsey Company 2020).
- **Complex Processes**: The buying, selling, and settlement of securities can be very long and cumbersome procedures (Gartner 2019).

3. **Risk Management**

Current Practices:

- **Reactive Approaches**: Risk management frequently includes reactive measures and offers little visibility into risk exposure in real time (KPMG 2019).
- **Data Fragmentation**: Risk data is dispersed through many systems and sources, thus making a comprehensive risk assessment difficult (Narayanan et al. 2016).

Blockchain Solutions for Investment and Wealth Management

1. **Enhanced Transparency and Data Integrity**

Overview:

- **Blockchain Solution**: It is one of the transparent, immutable ledgers solutions for the recordation of investment transactions and portfolio data. Thus, it prevents tampering and, therefore, fraud cannot be done (Christidis and Devetsikiotis 2016).
- **Benefits**: Increased openness and accuracy in investment records, meaning more trust among investors and asset managers (PwC 2020).

Example:

- **CurioInvest**: CurioInvest uses blockchain and avails transparent records of investments to enhance security, yet enables the monitoring of investments in real time by investors (CurioInvest 2021).

2. **Smart Contracts for Automated Transactions**

Overview:

- **Blockchain Solution**: Smart contracts can auto-invest transactions like buy/sell orders, dividend payouts, and portfolio rebalancing. These contracts automatically execute predefined rules, which minimizes manual intervention (Christidis and Devetsikiotis 2016).
- **Benefits**: It increased efficiency, reduced transactional costs, and ensured investment order executions were accurate (McKinsey Company 2020).

Example:

- **Synthetix**: Synthetix uses smart contracts to realize enforcement on automated trading activities for synthetic assets, thus making investment transaction efficiency higher (Synthetix 2021).

3. **Decentralized Investment Platforms**

Overview:

- **Blockchain Solution**: Direct person-to-person investment is allowed by blockchain-based investment platforms. An entity, avoiding the normal middlemen, can thereby reduce costs while creating easier access (Christidis and Devetsikiotis 2016).
- **Benefits**: Lower fees, faster transaction processing, and greater access to investment (PwC 2020).

Example:

- **Compound**: Compound is another noncentralized lending and borrowing platform in terms of cryptocurrencies, which enables actual peer-to-peer transactions (Compound 2021).

4. **Tokenization of Assets**

Overview:

- **Blockchain Solution**: Tokenization is described as the conversion of physical and financial assets, real estate, equities, or other investments into digital tokens on a blockchain (Christidis and Devetsikiotis 2016).
- **Benefits**: It increases the liquidity, fractional ownership and availability, hence making room for more access to investment opportunities (PwC 2020).

Example:

- **Real Estate Asset Tokenization**: Websites such as RealT tokenizes real estate assets such that investors can buy fractional ownership in properties (RealT 2021).

5. **Enhanced Risk Management**

Overview:

- **Blockchain Solution**: With the blockchain, real-time access and visibility within investment portfolios reduce the processes in risk management and decision-making (Christidis and Devetsikiotis 2016).
- **Benefits**: It more accurately and contemporarily captures the available risk exposures with associated controls (KPMG 2019).

Example:

- **Chainlink**: Chainlink provides decentralized oracles that provide real-time data to blockchain-based financial applications, thus enhancing risk management (BitRewards 2021).

6. **Efficient Settlement and Clearing**

Overview:

- **Blockchain Solution**: Blockchain can simplify the settlement and clearing of investment transactions by providing an efficient and reliable ledger to record trades and transfers (Christidis and Devetsikiotis 2016).
- **Benefits**: The settling time is less, low in cost, and easy operation (McKinsey Company 2020).

Example:

- **DTCC's Project ION**: DTCC is utilizing blockchain to improve post-trade settlement process efficiency with its Project ION (DTCC 2021).

Challenges and Considerations

1. **Regulatory and Legal Issues**

   - **Compliance**: Blockchain-based investment solutions must comply with financial regulations and legal requirements, which can change from jurisdiction to jurisdiction (KPMG 2019).

- **Regulatory Approval**: In a blockchain-based investment platform, regulatory approval could require some deep plunging into comparatively difficult legal and regulatory problems (Deloitte 2021).

2. **Integration with Traditional Systems**

   - **Compatibility**: Integrating blockchain solutions into existing systems, infrastructure, and investment management could not be more complex (Gartner 2019).
   - **Data Migration**: The investment data migrated to the blockchain platforms have to be secure and reliable (McKinsey Company 2020).

3. **Adoption and Education**

   - **Consumer Awareness**: Educating the investors and asset managers on the benefits and use of blockchain technology in investment management is very fundamental to adoption (PwC 2020).
   - **Industry Resistance**: There was resistance to new technologies and modified established practice in the industry. This could be quite a challenge (Christidis and Devetsikiotis 2016).

2.2.10.2 Risk Management and Derivatives Trading

Risk management and **derivatives trading** are the main ingredients of modern financial markets. While managing risk identifies, evaluates, and then reduces financial risks of assets and stable returns, trading derivatives takes care of buying and selling financial instruments that derive their value from one or more underlying assets in forms of stocks, bonds, commodities, or interest rates. Blockchain technology can do much to enrich the areas mentioned above by improving transparency, efficiency, and security.

Traditional Risk Management and Derivatives Trading.

1. **Risk Management**

Current Practices:

- **Manual Processes**: It mainly relies on manual processes and heterogeneous systems used to monitor and measure exposure to risk (Deloitte 2021).
- **Limited Real-Time Data**: Intraday systems can sometimes facilitate less real-time data, not able to show the ability to respond quickly to emerging risks (PwC 2020).

2. **Derivatives Trading**

Current Practices:

- **Centralized Exchanges**: Derivatives trading normally occurs on centralized exchanges, with all the related problems of delay, high cost, and counterparty risk (McKinsey Company 2020).

- **Complex Settlements**: The very process of settlement of derivative contracts is complex, involves multiple intermediaries, and increases costs along with chances of error (Gartner 2019).

Blockchain Solutions for Risk Management and Derivatives Trading

1. **Enhanced Transparency and Data Integrity**

Overview:

- **Blockchain Solution**: Blockchain provides an immutable and transparent record for the risk management data and for the transaction of derivatives. This increases the chances of data integrity and reduces fraud risks (Christidis and Devetsikiotis 2016).
- **Benefits**: Increased transparency and accuracy in risk assessments and derivative trades thus fostering trust and reducing possible disputes (PwC 2020).

Example:

- **Corda**: Corda is a blockchain platform optimized for financial services; it delivers transparent and secure records of transactions, which would improve the accuracy and integrity of risk management and derivatives trading (CurioInvest 2021).

2. **Smart Contracts for Automated Risk Management**

Overview:

- **Blockchain Solution**: The risk management process is automated by means of smart contracts including monitoring, trades execution, and collateral administration. It automatically implements predefined rules thus reducing drastically input from the human end (Christidis and Devetsikiotis 2016).
- **Benefits**: Enhance efficiency, decrease cost of operations and thus decrease error in risk management (McKinsey Company 2020).

Example:

- **OpenLaw**: OpenLaw uses smart contracts on blockchain, which automatically generates and executes derivative contracts and hence streamlines the process of trading (OpenLaw 2021).

3. **Decentralized Exchanges for Derivatives Trading**

Overview:

- **Blockchain Solution**: Decentralized exchanges (DEXs) enables peer-to-peer trading of the derivatives in a chain-based, intermediary-free configuration. This should reduce the cost and risk of counterparty (Christidis and Devetsikiotis 2016).
- **Benefits**: Higher access to markets, lower fees, and more security in derivative trading (PwC 2020).

Example:

- **dYdX**: dYdX is a decentralized platform of derivatives trading. An almost risk-free setting is provided while trading many financial instruments (dYdX 2021).

4. **Improved Risk Analytics and Monitoring**

Overview:

- **Blockchain Solution**: Blockchain technology will allow real-time access to data and analytics in risk management. This is through an enhanced monitoring and measuring of exposures (Christidis and Devetsikiotis 2016).
- **Benefits**: The strong awareness and reaction toward new risks will uncover better, more timely data (KPMG 2019).

Example:

- **Chainlink**: Chainlink provides decentralized oracles used in risk management applications of blockchain, thereby supplying real-time data to enhance the accuracy of risk appraisals (BitRewards 2021).

5. **Streamlined Settlement and Clearing**

Overview:

- **Blockchain Solution**: With a derivatives contract, blockchain may make settlement and clearing easier as it can safely record trades and transfers (Christidis and Devetsikiotis 2016).
- **Benefits**: Settlement faster, cheaper, and more effective operating time (McKinsey Company 2020).

Example:

- **DTCC's Project ION**: DTCC's Project ION uses blockchain in the implementation of a much faster service of post-trade settlement for derivatives (DTCC 2021).

6. **Collateral Management and Optimization**

Overview:

- **Blockchain Solution**: Blockchain allows for the real-time management of collateral assets through a tamper-proof, immutable, and transparent ledger record of usage and collateral assets (Christidis and Devetsikiotis 2016).
- **Benefits**: More efficient management of collateral, less risk to dispute, and more transparency (PwC 2020).

Example:

- **HQLAX**: HQLAX uses blockchain technology to enhance collateral management processes so that collateral assets can be managed more effectively and transparently (IBM Research 2021).

Challenges and Considerations

1. **Regulatory and Legal Issues**
    - **Compliance**: Blockchain-based derivatives trading solutions have to comply with all existing financial regulations and legal requirements (KPMG 2019).
    - **Regulatory Approval**: The governmental approvals for blockchain-based solutions take a long and laborious process (Deloitte 2021).
2. **Integration with Traditional Systems**
    - **Compatibility**: Interfacing with trading and risk management systems may be highly capital-intensive and technologically intensive for blockchain technology (Gartner 2019).
    - **Data Migration**: It includes data migration. Data from the traditional systems must be migrated into safe and accurate blockchain platforms (McKinsey Company 2020).
3. **Adoption and Industry Resistance**
    - **Consumer Awareness**: Educating market participants about the advantages and application of blockchain technology in derivatives trading is the most important adoption (PwC 2020).
    - **Industry Resistance**: Industrial change is tough as new technologies and newer practices have created resistance in industrial settings (Christidis and Devetsikiotis 2016).

2.3 Research Gaps in Blockchain Applications in the Banking Sector

Blockchain technology can change the game in banking on all fronts-from transaction processing and compliance to customer service. However, as shown below, there are still research gaps that need to be covered in addressing the challenges blockchain technology has for the banking sector as a whole:

1. **Scalability and Performance**

Issue:

- **Transaction Speed and Capacity**: The existing blockchain systems mainly on the public networks have been characterized as slow and low throughput for transactions. Which may grossly compromise high-frequency operations in the banking departments (Buterin 2020a, b).
- **Research Gap**: Scalable blockchain solutions for large support of a high quantity of transactions are characteristic of banking applications without impacting performance adversely.

2. **Integration with Legacy Banking Systems**

Issue:

- **Legacy Infrastructure**: Superimposing blockchain on the existing conventional banking infrastructure and legacy systems is quite elaborate and costly (Gartner 2019).
- **Research Gap**: Interoperability solutions for the interaction of blockchain technology with existing banking systems must be designed using standards and middleware.

Issue:

- **Regulatory Uncertainty**: Rules and regulations around blockchain usage in banking is still evolving, and its current integration into the pre-existing financial regulations is unknown (KPMG 2019).
- **Research Gap**: There is a need to establish clear regulatory guidelines and compliance mechanisms for blockchain applications in banking to ensure legal and regulatory compliance.

3. **Data Privacy and Security**

Issue:

- **Privacy Concerns**: The use of blockchain could be in variance with the requirement for keeping certain data as confidential in a bank (Narayanan et al. 2016).
- **Research Gap**: Fill up this research gap using a privacy-preserving technology and mechanisms of zero-knowledge proof on confidential transactions.

4. **Smart Contract Vulnerabilities**

Issue:

- **Security Risks**: Coding errors or vulnerabilities in smart contracts may lead to the smart contracts exposing risks of financial consequences or enterprise operational disruption in applications like banking (Christidis and Devetsikiotis 2016).
- **Research Gap**: Significant methods of developing, auditing, and securing smart contracts need to be improved for higher reliability and safety in banking applications.

Issue:

- **Resistance to Change**: The cause of the acceptance of blockchain technology in banks is tradition, the cost involved in implementing new technologies, and doubt in new technology (PwC 2020).
- **Research Gap**: New strategies have to be found and developed through education of stakeholders and pilot programs.

5. **Interoperability Between Different Blockchain Platforms**

Issue:

- **Ecosystem Fragmentation**: Blockchains are largely siloed, self-contained economies that are not structured to interoperate or exchange data with other blockchains (BitRewards 2021).
- **Research Gap**: Interoperability standards and protocols for seamless communication and data transfer among different blockchain systems, also a gaping holed.

6. **Cost of Implementation**

Issue:

- **High Implementation Costs**: Intensive implementation processes: The cost related to the implementation processes of blockchain technology involves technological development, infrastructure, and training costs (McKinsey Company 2020).
- **Research Gap**: Determines determinant factors, and cost-effective ways of expenditure-cutting that may induce its eventual use in banking.

7. **Blockchain-Based Customer Experience Enhancementsz**

Issue:

- **User Experience**: Despite better security and efficiency, effects on broader customer experience and quality of banking services are still unseen with blockchain (Deloitte 2021).
- **Research Gap**: The existing research gap refers to how blockchain can be utilized to improve customer service and experience in offering banking services, especially usability and customer satisfaction.

8. **Risk Management and Fraud Prevention**

Issue:

- **Fraud Risks**: Prevents fraud possibility but gives rise to new prospects of risk and vulnerabilities (Accenture 2020).
- **Research Gap**: There is a research gap in designing a risk management and fraud-prevention framework specific to blockchain applications in banking.

Given these research gaps, applying blockchain technology in banks would be very crucially needed. Scaling, integration, conformity to regulations, privacy, security, and adoption difficulties will significantly enhance the banks' operations and services through embedding blockchain technologies.

2.4 Need for Better Solutions

However, innovations and inventions in application implementation will still be required to fill the yet ongoing research gaps identified within blockchain applications for banking. Some of the major areas where a better solution needs to arise are:

1. **Scalability Solutions**

Need:

- **High Transaction Throughput**: Blockchain solutions require a fast execution capability to process high volumes of transactions.
- **Solution**: It leads to blockchain architecture development, such as sharding; deploy layer-2 scaling solutions like state channels, rollups; and consensus algorithm refinements for extensibility and higher throughput.

Example:

Ethereum 2.0 project scales by helping achieve the shift away from Proof of Work, to Proof of Stake (PoS) and the integration of a so-called concept dubbed sharding.

2. **Integration Frameworks**

Need:

- **Seamless Integration**: Banks require very robust frameworks that integrate blockchain with existing legacy systems and financial infrastructure seamlessly.
- **Solution**: Middleware solutions, APIs, and integration platforms that will make blockchain-based systems easily interface with the traditional banking system.

Example:

Hyperledger Fabric allows users to integrate with existing modular architectures.

3. **Regulatory Compliance Solutions**

Need:

- **Clear Guidelines**: The maze of changing regulatory challenges for blockchain applications in banking.
- **Solution**: Create fully comprehensive regulatory frameworks for blockchain, along with tailored compliance tools, which may include the automation of monitoring and reporting about compliance.

Example:

Some of the guidelines provided by the Financial Action Task Force (FATF) include cryptocurrencies, blockchains, and recommendations that go by in terms of anti-money laundering (AML) standards.

4. **Privacy-Preserving Technologies**

Need:

- **Data Confidentiality**: That would mean private financial information is obscured on the blockchain.
- **Solution**: Privacy-enabling technologies, which include zero-knowledge proofs, ring signatures, and confidential transactions.

Example:

zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) for transactional privacy.

5. **Smart Contract Development and Security**

Need:

- **Reliable Smart Contracts**: Smart contracts must be trustworthy, non-buggy, and capable of handling intricate banking processes.
- **Solution**: It should advance developer tools for smart contracts, full testing frameworks, and automation of audit solutions of security.

Example:

Tools like MythX and Securify automatically scan for smart contract security analysis.

6. **Overcoming Adoption Barriers**

Need:

- **Enhanced Adoption**: Proof of skepticism and resistance of the banking sector towards blockchain technology.
- **Solution**: Stakeholder education, pilot projects; demonstration of value via blockchain through case studies and practical use cases.

Example:

Some active consortia on adoption and standardization in blockchain include R3 as well as the Enterprise Ethereum Alliance (EEA).

7. **Interoperability Solutions**

Need:

- **Cross-platform Compatibility**: The interaction between various blockchain platforms.
- **Solution**: Cross-chain protocols and interoperability solutions that enable multi-blockchains to communicate with each other.

Example:

Polkadot and Cosmos are blockchain-based ecosystems that establish an interoperability framework among other blockchains.

8. **Cost-Effective Implementation**

Need:

- **Reduced Costs**: The cost of financial and operational cost went down due to blockchain.
- **Solution**: Researching and investigation of cost-effective blockchain solutions—that is, open-source platforms, streamlining blockchain infrastructure and its processes.

Example:

Cloud-based blockchain services like IBM blockchain and AWS Managed blockchain can minimize the cost of infrastructure.

9. **Enhancing Customer Experience**

Need:

- **Improved Service**: Using blockchain to serve customers better across the entire banking experience.
- **Solution**: More friendly user interfaces, better integration of customer care support and blockchain applications in the banking stream.

Example:

Blockchain-based wallets and identity verification systems enhance customer onboarding and transaction experiences.

10. **Risk Management and Fraud Prevention**

Need:

- **Effective Risk Management**: Proper risk management and fraud prevention through blockchain.
- **Solution**: Advanced fraud-detection systems, a risk management framework, and blockchain-based monitoring tools among others.

Example:

Blockchain-based systems eliminate and handle all risks through fully transparent auditing and real-time monitoring.

All these requirements will push banks forward to innovation solutions and technological breakthroughs. Scalability, integration, regulatory compliance, privacy, security, adoption, interoperability, cost-effectiveness, customer experience, and risk management are the parameters, which will define how the banks will implement blockchain successfully to their benefit and in that way enhance the operations and the deals they offer with their customers.

2.5 Banking Applications of IoT, AI, and Blockchain

The rejuvenation of the **Internet of Things (IoT)**, **Artificial Intelligence (AI)**, and **blockchain** technologies has transformed the financial and banking industries. It brings together a range of applications that promise efficiency and security in a host of applications and, most importantly, improvements in customer experience to financial institutions. A tour of how the confluence of IoT, AI, and blockchain applies in the finance and banking sector follows:

2.5.1 Enhanced Fraud Detection and Prevention

AI and **blockchain** combined with **IoT** could be a strong system for **fraud detection and prevention**. IoT devices bring real-time data of transactions, while the same data is used by AI algorithms to decide anomalies. Such fraud would be harder to commit and easier to track because blockchain technology will ensure the keeping of a record of all the transactions securely and unchangeably. For example, AI-based technology will leverage the data of IoT for the detection of anomalies in transaction behavior, and blockchain will, instead build up a transparent non-editable record of each transaction (Deloitte 2020)

2.5.2 Smart Contracts for Automated Processes

Smart contracts on the **blockchain** automate all the banking procedures from the lending procedure approval to the claims of insurance. These contracts self-execute automatically whenever particular conditions are met. This is why the IoT devices coupled with AI have to happen in real time for the breaking of these triggers: it facilitates simpler procedures which are a result of reducing human interference and bring out a maximum level of efficiency in the execution of tasks (IBM Research 2021).

2.5.3 Predictive Analytics and Risk Management

AI employs **IoT** data for **predictive analytics** in risk management. The products of IoT can gather real-time diversity, whether it is real-time markets or the behavior of the customers. AI models analyze the data to ensure what might happen ahead and what patterns could develop. Blockchain thereby enhances this with the authenticity of tamper-proof data going into the making of predictions. For example, predictive models of market risk or creditworthiness of customers would be quite more productive when integrated with the appropriate data from sensors from IoT and secure storages in blockchains (McKinsey Company 2021).

2.5.4 Customer Identity and Authentication

Blockchain is a secure, decentralized place for conducting **digital identity management**. **IoT** devices can collect and authenticate user data, while AI systems can analyze this data for the affirmation of identity. For instance, an identity verification system via blockchain may receive biometrics from IoT sensors to process using AI algorithms, thus concluding the affirmation of users. This will enhance security and minimize fraudulent activities since customer identities are protected (Zhang et al. 2016; Zhao et al. 2018; Zohar 2015; Zcash 2021; Winding Tree 2018; World Bank 2020; Yearn.Finance 2021).

2.5.5 Decentralized Finance (DeFi)

In a **DeFi** System **blockchain** facilitates the decentralization of financial systems. It also provides optimization of trading strategies, and further helps in analyzing market data. **IoT** devices can give real-time updates regarding market conditions as well as the status of assets. This system provides more transparent and efficient financial transactions and investments. For instance, **AI** algorithms may optimize asset allocation based on the real-time data collected by IoT. Blockchain ensures that all transactions are secure and transparent (EY 2021).

2.5.6 Automated Trading and Portfolio Management

Integration of **AI** and **blockchain** enhances the **automated trading** and **portfolio management**. **IoT** devices provide the real-time market data that the AI system analyzes and bases the trading decision and portfolio management. Blockchain technology ensures the precise recording and safe of all trades and transactions. Thus, the integration type would ensure higher accuracy and efficiency in trading strategies and portfolio management (Filecoin 2021).

2.5.7 Supply Chain Finance

Blockchain presents true transparency and traceability in **supply chain finance**, and **IoT** sensors monitor the movement and condition of goods. **AI** processes such streams of data to maximize financing decisions and minimize risks. For example, an IoT sensor may track in-transit goods and their condition. Then, AI can process such data to review terms of financing or to identify preemption issues. Thus, all data is therefore secured and cannot be changed, and hence, provides a reliable record for all transactions carried out (PwC 2019).

2.5.8 Customer Experience Enhancement

AI and **IoT** provide more **enhance customer experiences** through personification with services and interfaces. **Blockchain** creates safely and transparently the record of customer interaction and preference. For instance, using real-time data of IoT devices, AI-driven chatbots can offer personalized financial advice whereas blockchain supports to maintain and provide customer information securely and only to the authorized ones (Gartner 2021).

2.5.9 Regulatory Compliance

Blockchain helps keep **regulatory compliance** in check owing to its transparent, immutable transaction records. The **AI** goes through such data to understand instances of non-compliance with regulations and **IoT** appliances perform real-time observations over financial transactions. Such integration makes compliance reporting a smooth sailing affair, and the risk of regulation breaches reduces (Deloitte 2020).

AI and blockchain technologies are immense transformation opportunities for changes in the financial and banking sectors. The technologies will attract into an existence real-time data gathering in the intelligent analysis and safe recording of transactions to provide new solutions, make it efficient, secure and customer-convenient. These applications will keep growing and transforming the financial industries as new avenues will appear to address those challenges and exploit the spaces left unexploited.

2.6 Case Studies: Blockchain, IoT, and AI in Banking and Financial Sector

Applications of such technologies in real-life examples for the financial sector can give a clue about their economic effects. Following are the case studies of practical examples of how blockchain, IoT, and AI are applied to developing and improving financial services and banking.

Real-World Examples of Blockchain, IoT, and AI in the Finance.

2.6.1 Blockchain in Cross-border Payments

Case Study: **Ripple and Santander**

- **Background**: Ripple, a blockchain-based payment platform, collaborated with Santander to simplify cross-border payments.
- **Implementation**: Ripple's technology enables fast, inexpensive, and more efficient cross-border money transfers using its digital asset called XRP as well as a distributed ledger.
- **Impact**: Transaction times were reduced from days to seconds, with transaction fees far lower than could be achieved with traditional banking approaches.
- **Outcome**: The customers of Santander enjoyed faster payments and lesser costs, showing promise in blockchain for transforming cross-border payments.

2.6.2 IoT for Real-Time Financial Data

Case Study: **IBM and TradeLens**

- **Background**: IBM and Maersk launched the blockchain-based joint venture called TradeLens, which is aimed to increase transparency in global supply chains.
- **Implementation**: IoT devices can gather data from shipping containers in real time and feed this information into TradeLens, which is maintained on a blockchain to provide an ultimate proof of one, single version of the truth for all parties concerned.
- **Impact**: This real-time data integration improves the accuracy of financial forecasting, inventory management, and logistics planning. It also reduces fraud and operational inefficiencies.
- **Outcome**: With TradeLens, the process of supply chains becomes more effective with better financial decisions created by more accurate time data.

2.6.3 AI in Credit Scoring

Case Study: **Zest AI**

- **Background**: Zest AI utilizes artificial intelligence to enhance credit scoring models and compute credit-worthiness.
- **Implementation**: Zest AI utilizes machine learning algorithms to draw data from a wide variety of sources, including non-traditional ones, to create the most complete and accurate credit score.
- **Impact**: Lenders will be able to loan to a larger customer base. That would include those who never had any credit history; therefore, lowering the chance of default.
- **Outcome**: Increased credit to the disadvantaged provides access and better accuracy in risk assessment for the lender.

2.6.4 Blockchain for Digital Identity Verification

Case Study: **SelfKey**

- **Background**: Overview SelfKey is a decentralized platform based on blockchain that will make digital identity verification safe.
- **Implementation**: This also improves the privacy and security provided at the same time also simplifies the KYC process of financial institutions.
- **Impact**: This approach enhances privacy and security while simplifying the KYC (Know Your Customer) process for financial institutions.
- **Outcome**: Increased efficiency in the onboarding process. Efficient control of users over private data

2.6.5 AI for Fraud Detection

Case Study: **Darktrace and HSBC**

- **Background**: HSBC Forms Partnership with Darktrace for AI-Powered Fraud Prevention Cybersecurity Solution.
- **Implementation**: Darktrace's machine learning systems monitor real-time anomalous patterns of financial transaction or network activity that might indicate fraudulent activities.
- **Impact**: It detects fraud much earlier, and in comparison with the traditional method, there are fewer false positives.
- **Outcome**: High degree of safety measure and fewer fraudulent transactions for HSBC.

2.6.6 IoT in Asset Management

Case Study: **IBM and the City of Miami**

- **Background**: IBM, in collaboration with the City of Miami, developed a suite of IoT solutions for smart asset management and city planning.
- **Implementation**: IoT sensors report on the city's assets, which happen to be either infrastructure or environmental conditions. The analysis leads to optimizing their management and maintenance.
- **Impact**: It will bring about better asset management decisions and predictive maintenance besides providing real-time city planning.
- **Outcome**: Efficient resource handling in towns, and provision of quality services.

2.6.7 Blockchain for Trade Finance

Case Study: **HSBC and Standard Chartered**

- **Background**: HSBC and Standard Chartered launched a blockchain-based commercial paper trading platform very recently.
- **Implementation**: The use of blockchain in the digitization and automation of any kind of trade finance-from letters of credit to documents.
- **Impact**: Smoothing out trade finance operations, less paperwork, greater transparency and efficiency.
- **Outcome**: Much faster and safer trade finance transactions for the banks and their customers.

2.6.8 AI in Investment Management

Case Study: **BlackRock's Aladdin**

- **Background**: The firm also has deployed the AI and machine learning investment management and risk assessment tool Aladdin from BlackRock.
- **Implementation**: Aladdin analyzes enormous databases of markets, models risks, and aids investment decisions by using AI-driven insights.
- **Impact**: With better precision in predictive risk, actual investment strategies and thus positive financial outcomes for the investors.
- **Outcome**: Improved investment performance, and better decision-making.

This clearly manifests how blockchain, IoT, and AI are being used to bring revolutions and changes in every aspect of the finance sector. Real-life problems are addressed with practical application, which will help improve efficiency, security, and the decision-making process for financial services.

Real-World Examples of Blockchain, IoT, and AI in Banking.

2.6.9 Blockchain in Banking

Case Study: **JPMorgan Chase and JPM Coin**

- **Background**: JPMorgan Chase is the world's largest bank that designed and launched JPM Coin-an in-house blockchain-based digital currency.
- **Implementation**: This can be done at any time with prompt, safe, and transparent transfers between institutional clients. It also uses JPMorgan's private blockchain to implement this transfer.
- **Impact**: With the advent of cross-border transactions, such effectiveness is enhanced because settlement times are reduced from days to mere seconds.
- **Outcome**: Improved Liquidity management and operational efficiency of institutional clients another testimony to the potential of blockchain streamlining banking processes.

Case Study: **Bank of America's Blockchain Patents**

- **Background**: Bank of America has seriously invested in blockchain technology by filing several patents related to blockchain applications in banking.
- **Implementation**: Blockchain under patents, including highly secure transactions, monitoring compliance, and digital asset management.
- **Impact**: Such innovations are meant to have better transaction security, fraud reduction, and improved regulatory compliance.
- **Outcome**: Bank of America's blockchain patents indicate the bank's interest in observing and implementing blockchain for different banking-related activities.

2.6.10 IoT in Banking

Case Study: **BNP Paribas and IoT-Based Asset Management**

- **Background**: The bank has used the Internet of Things to enhance asset management and improve operational efficiency.
- **Implementation**: It utilizes IoT sensors to monitor and manage physical assets such as ATMs and infrastructures of branches. Such has absolute real-time information on the conditions and performance of the asset.
- **Impact**: The IoT-based system allows for predictive maintenance. Thus, it reduces the downtime and raises banking services' reliability.
- **Outcome**: Improve operational efficiency and save costs on account of better management of assets and reduced maintenance requirements.

Case Study: **CaixaBank's IoT Solutions for Branch Operations**

- **Background**: Main Spanish Bank CaixaBank has adapted IoT solutions to the optimization of its branches' operations.
- **Implementation**: IoT devices monitor environmental conditions and foot traffic in branches, thus gathering statistics and information to optimize energy usage, staffing, and customer service.
- **Impact**: Enhanced branch efficiency and better customer experience through the implementation of process changes using data-driven insights.
- **Outcome**: It would result in better management of branches and good relations with customers.

2.6.11 AI in Banking

Case Study: **HSBC and AI-Powered Fraud Detection**

- **Background**: HSBC uses AI and ML for the detection and prevention of fraud.
- **Implementation**: HSBC's AI scans the transactions and identifies any odd-behavioral patterns together aggregating to potential frauds.
- **Impact**: The system works successfully to enhance the reliability of fraud detection while reducing false positives, thus securing the bank and its customers.
- **Outcome**: With proper security systems and decreasing frauds, customers shall be confident and the operations will be successful.

Case Study: **Wells Fargo's AI-Based Customer Service**

- **Background**: For instance, Wells Fargo uses AI to enhance customer service through chatbots and virtual assistants.
- **Implementation**: AI Virtual Assistants process relatively routine and simple customer questions and transactions while leaving more complex work to the human representatives.
- **Impact**: More efficient customer service order processing and a higher rate of customer satisfaction due to shorter turnarounds.
- **Outcome**: It will feature improved customer experience and operational efficiency in AI services.

Blockchain and IoT, AI usage at the banks: It increases efficiency in use as well as in security aspects coupled with enhanced customer experience. It offers a pathway for the upgrade of the operational sectors of banking to efficiently streamline transactions, improve asset management, and extend to fraud detection and excellent customer service.

2.7 Open Issues

2.7.1 Banking Sectors

Most open issues arise in relation to the implementation and use of efficiency as blockchain, IoT, and AI advance. Such an issue will help maximize the use of such technologies in the banking sector.

2.7.1.1 Scalability Challenges

Blockchain Scalability:

- **Issue**: Most blockchains in applications of banking have low scalability. Some of the issues include low transaction throughput and slow processing. This is rather a scaling limit for usability on large scales.
- **Impact**: All this puts the limelight on several limitations that may slow or bring costs in these volumes, hence tending to inefficiency in banking activity.
- **Need**: Better blockchain scalability solutions, such as sharding and layer-2 solutions, including lightning network, in addition to advanced consensus mechanisms.

IoT Data Management:

- **Issue**: As IoT devices increase so dramatically in number, a massive amount of data is produced. The management and storage of such information become difficult.
- **Impact**: Inefficient data handling leads to delayed information processing as well as storage at high costs.
- **Need**: To ensure integration of real-time analytics and edge computing capabilities.

2.7.1.2 Regulatory and Compliance Issues

Regulatory Uncertainty:

- **Issue**: The blockchain, IoT, and AI regulatory regime is in the midst of evolution and significantly differs across jurisdictions.
- **Impact**: It would result in a drag in adoption and increased costs for compliance for financial firms.
- **Need**: An urgent need for globally standardized regulatory frameworks that offer clarity and consistency.

Compliance Complexity:

- **Issue**: Using the blockchain, IoT, and AI in banks needed to comply with existing financial regulations that are pretty clumsy.
- **Impact**: The entry of new technologies would prevent the shift in bank operations to the issues of regulations.
- **Need**: Automated compliance tools and strategies to match new technologies with regulatory standards.

2.7.1.3 Security and Privacy Concerns

Blockchain Security:

- **Issue**: This technology makes blockchain really robust and secure, but not invulnerable to attacks and weaknesses such as bugs in the smart contracts and 51% attacks.
- **Impact**: Money loss, along with the loss of trust in blockchain technologies.
- **Need**: Innumerable research on new subtlety techniques as well as security practices and improvement of blockchain systems.

IoT Privacy:

- **Issue**: This IoT device may expose itself to breaches, thus raising certain data privacy and security issues.
- **Impact**: Sensitive data generated by IoT is prone to breach privacy and loss of money.
- **Need**: Establish robust security protocols and privacy-protecting technologies for IoT systems.

4. **Interoperability Challenges**

Cross-platform Integration:

- **Issue**: The interconnection of blockchain and IoT with AI across multiple platforms and systems poses a lot of complicated work and interoperability problems.
- **Impact**: Non-working in an interoperable nature might stop entirely integrated systems from running very smoothly and limit technology solutions from reaching full efficiency.
- **Need**: Standardized protocols and frameworks for better integration and interoperability.

Data Standardization:

- **Issue**: In the absence of commonly agreed data standards, it may become challenging to exchange and append data from other systems.
- **Impact**: The inconsistent data formats may interfere with data sharing and analysis properly.

- **Need**: Research on data normalization using an inter-system protocol that can result in very high levels of interoperability.

2.7.1.4 Ethical and Social Implications

AI Bias:

- **Issue**: AI systems inherit and perpetuate biases, with discriminatory results against other providers of financial services.
- **Impact**: Unfair treatment to the customers due to biased AI algorithms coupled with increased regulatory scrutiny.
- **Need**: Studying developing such transparent and fair AI models to avoid discrimination.

Impact on Employment:

- **Issue**: Some of the potential effects of increasing automation with AI and blockchain technologies will include job displacement and changes in the employment trend.
- **Impact**: Automation can affect employment levels and job roles, requiring strategies to manage the transition.
- **Need**: Socio-Economic impacts of Automation and Integrated strategy for Workforce Transition and Retraining: a research paper.

2.7.1.5 Integration with Traditional Systems

Legacy Systems:

- **Issue**: Most of these banks rely heavily on legacy systems, which are not very easily integrated into new blockchain, IoT, or AI.
- **Impact**: Integration problems symbolize high cost and operational loss.
- **Need**: Hybrid solutions should have in-depth analysis, and best practices in introducing new technology with legacy systems.

Transition Strategies:

- **Issue**: Design appropriate transfer mechanisms into new technology that will not bother the current activities.
- **Impact**: For instance, uncontrolled transitions may lead to operationally and cost-increasingly inefficient practices.
- **Need**: Validation of transition management frameworks and tools that provide support for effective integration and adoption.

2.7.1.6 Cost and Resource Constraints

Implementation Costs:

- **Issue**: Cost of deployment and operation: Blockchain, IoT, and AI are somewhat cost-intensive that might become a problem for some of the institutions.
- **Impact**: These technologies are likely to be costly to implement, mainly for the small-sized banks.
- **Need**: Find cost-effective alternatives and models to shave off installation and running costs.

Resource Requirements:

- **Issue**: The operational requirement of the need for expensive computational resources and technical know-how limits high tech.
- **Impact**: Given the resource constraints, banks would not be able to fully utilize blockchain, IoT, and AI solutions.
- **Need**: Algorithm development with more efficient usage and optimization of resources.

Such open problems and issues need to be solved with quick solutions to enable swift adoption and the benefits of such blockchain, IoT, and AI technologies in banks and banking institutions. Such research directions for innovation science on scalability, regulatory compliance, security, interoperability, ethics, system integration, and cost management wouldn't be very easy to make mainstream reality.

2.8 Future Research Prospects

2.8.1 Banking Sectors

The banking area is among the most outstanding industries affected by the incorporation of technology. Technologies such as blockchain, IoT, and AI promise to revolutionize most processes in the area. However, much research still has to be conducted to further realize the full potential of these technologies in banking. Some of the future potential for research is in the following areas:

2.8.1.1 Blockchain Scalability for Banking Transactions

- **Problem**: All existing blockchain systems lack scalability in processing large numbers of transactions usually required in banking, especially for cross-border payments and real-time settlements.

- **Research Prospect**: Improvement of blockchain Scalability. New variants of consensus algorithms, like Proof of Stake, Layer 2 solutions, or sharding or off-chain processing, are possibilities. Hybrid architectures for public and private blockchain in banking, ensuring high performance and security.
- **Impact**: Scaling up will make blockchain approachable to all banking applications in the forms of remittances, real-time payment processing, and settlements.

2.8.1.2 Regulatory and Compliance Frameworks for Blockchain in Banking

- **Problem**: The development of the blockchain application in banking was surrounded by an ever-changing regulatory landscape and, therefore, uncertain application of these technologies.
- **Research Prospect**: The future scope in the research of standardized frameworks that can be globally accepted in the context of compliance and aimed towards blockchain-based banking services includes KYC (Know Your Customer), AML (Anti-money Laundering), along with real-time monitoring through AI and blockchain.
- **Impact**: This will help the banks increase clarity in their definition of the regulatory frameworks and then avoid compliance risks effectively for further adaptability on blockchain in secure and transparent banking operations.

2.8.1.3 AI-Driven Fraud Detection and Risk Management

- **Problem**: There are plenty of applications and implementations of AI in fraud detection and risk management, but it needs a much more sophisticated model to adapt in real time to the newly emerging threats in the world of banking.
- **Research Prospect**: It has to be designed with a future perspective in terms of AI models to predict and prevent fraud as they occur. The features can include integration of blockchain technology recording immutable transactions thereby increasing overall security and transparency.
- **Impact**: With the newly AI-powered fraud detection, the probability of fraud would dwindle down, and so will operational efficiency and an increase in customers' trust in banks.

2.8.1.4 Interoperability of Blockchain Systems in Banking

- **Problem**: Banks are present on numerous blockchain systems so can't even check or create an effortless cross-border transaction.
- **Research Prospect**: Interoperability protocols on blockchain systems for banking-one promising area of future research could be the development of rules allowing for secure communication and interoperability between different

blockchains even without central mediaries or even via cross-chain bridges with decentralized oracles.
- **Impact**: Increased interoperability would allow for seamless global banking operations in areas like international payments, clearing, and settlement processes.

2.8.1.5 AI-Powered Personalization of Banking Services

- **Problem**: Current banking services often lack personalized experiences tailored to individual customer needs, which can affect customer satisfaction.
- **Research Prospect**: There should be considerable research done in the development of AI systems that would track real-time customer behavior and preference for customized banking products and services. The data from IoT devices, customer transaction history, and social media sites would be included by the AI system; the users get relevant advice on finance, loan products, and savings plans.
- **Impact**: AI-driven personalized banking services will increase customer engagement, satisfaction, and loyalty, and consequently, there will be better financial products available through these banks.

2.8.1.6 Blockchain for Decentralized Banking Services

- **Problem**: Traditionally and reflexively, people always depend on rigid centralized infrastructure that is not efficient and has single points of failure.
- **Research Prospect**: Models for Decentralized Finance-Based Banking Services may well Eliminate Intermediaries. Models can be released through decentralized lending, savings, and payment platforms using smart contracts on blockchain.
- **Impact**: Decentralized banking services might allow customers more freedom in exercising their access to funds, reduce transaction costs, and enable speedy transactions without the bias of third-party banking service intermediaries.

2.8.1.7 IoT Integration for Real-Time Banking Services

- **Problem**: While IoT is applied for real-time data collection in almost every industry, the use of applications for automatic financial services in the banking sector is almost senseless.
- **Research Prospect**: There could be a good prospect for future research on how the IoT devices can be integrated with the systems of the banks to enable services such as real-time scoring of credits, automated loan approvals, asset tracking, and continuous data streams that enable more insightful lending decisions and give real-time risk assessments.
- **Impact**: Integration of IoT in banking services improves its responsiveness and makes data-driven decisions that improve customer experiences and operational efficiency.

2.8.1.8 Data Privacy and Security in AI and Blockchain Systems

- **Problem**: Data privacy and security issues continue to endure despite the increased adoption of AI and blockchain technologies by banks, especially in financial data as well as personal data.
- **Research Prospect**: The envisaged future research likely is related to privacy-preserving technologies, such as zero-knowledge proofs and homomorphic encryption besides blockchain-based identity management solutions for secure authentication of customers and data sharing.
- **Impact**: This strength in data will add confidence in consumers' minds and result in the bold introduction of AI and blockchain technologies with clear guardrails of compliance and security in place.

2.8.1.9 AI and Blockchain for Real-Time Regulatory Compliance

- **Problem**: This is an issue about the rise in regulatory pressure on the banking system especially with regard to anti-money laundering (AML) and combating the financing of terrorism (CFT) standards.
- **Research Prospect**: The possibility of tracking every transaction and marking down every unusual one in real time can be well fitted in developing AI and blockchain-based systems that may automate compliance reporting and auditing processes, let regulatory adherence turn more effective, and man-reliant on errors.
- **Impact**: With the system combining AI and blockchain, the risks associated with regulatory relations will be drastically reduced, and hence the banks will save a lot of resources while following the stringent regulations.

Tomorrow's banks will look up towards scalability, regulatory frameworks, interoperability, privacy, and security to scale up the advantages of blockchain, IoT, and AI. Huge scope for research in these niche streams relevant to the banking industry with regards to innovations related to risk management, customer services, regulatory compliance, and decentralized financial services.

2.9 Recommendations

2.9.1 Banking Sectors

The recommendations for the actualization of blockchain, AI, and IoT in the finance and banking space are starting to emerge in varying forms—scalability, security, interoperability, regulatory compliance as well as how the new systems integrate with the old systems.

1. **Blockchain Integration and Scalability Improvements**

For instance, on the very same day, they would need blockchain systems with a distributed architecture that can process millions of transactions daily, in real-time settlements, and payment processing. Hybrid architectures of public and private blockchains would be needed so as to be secure but scaled.

2. **Strengthening Regulatory Compliance and Security**

Banks must ensure that blockchain-based banking applications adhere to emerging regulatory standards. They should develop solutions that automatically track and document transactions, improving real-time regulatory reporting and reducing human error.

3. **Enhance AI and IoT Adoption for Personalization and Risk Management**

As an example, the concept can help a bank design much more tailored loans and savings accounts that are well-informed by AI analytics. The systems of AI-based fraud detection integrated with IoT might possibly provide insight into real-time fraudulent activities with quicker response times.

4. **Improve Interoperability Across Blockchain Systems**

Banks would need to invest in researching interoperability solutions for blockchain-based banking services, so real-time cross-border transactions can be made possible and seamless interlink of other financial systems occur.

5. **Privacy-Enhancing Technologies**

Banks have to establish very robust encryption and deploy blockchain-based identity management solutions to protect sensitive customer data. Privacy-preserving technologies will increase confidence in the usage of blockchain-based financial services.

6. **Decentralized Financial Services (DeFi) Integration**

The banks can offer decentralized banking models that reduce operational costs and transaction times, thereby allowing services like peer-to-peer lending as well as automated loan agreements using smart contracts.

7. **IoT-Driven Real-Time Financial Services**

Banks should use it for real-time credit scoring and loan risk analysis by integrating data feeds from various sources such as smart devices and customer interfaces. This would enhance credit-making decisions and render processes more consistent for approvals.

8. **Foster Collaboration and Innovation Hubs**

Banks would have to invest in partnerships with fintech companies, academia institutes, and the blockchain start-ups to develop innovation in blockchain-based banking services. Joint ventures can speed up the process of developing both scalable and secure banking solutions.

9. **Educating Workforce and Stakeholders**

Such interlinkages of blockchain, AI, and IoT with banks must be informed to the workforce and stakeholders about its impact, advantages, and challenges. An informed workforce is the first ever requirement for incorporating new technologies into bank operations.

10. **Real-Time Fraud Detection and Prevention Systems**

For this, banks should work on the development of AI and blockchain-based fraud-detection tools regarding transactions, inconsistent patterns flagged, and interventions automatically set in real time.

Thus, the finance and banking sector is one of the best sectors placed to change the growth metrics with blockchain, AI and IoT as the actual pivots of innovation. It means banks and financial institutions really go about servicing their offerings by streamlining scalable aspects, security and compliance within a regulatory framework—bring them really in line, thus enabling build-up of trust in clients.

2.10 Ending Note

One salient landmark of the timeline of the **banking sectors** is **blockchain**, **AI**, and **IoT** integration. Such technologies open unprecedented opportunities to perfect efficiency, transparency, security, and innovation at an unexampled scale. Therefore, while advancing further, it will become indispensable in these sectors to make use of each's strengths in order to cross-overcome the challenges they are now facing **regulatory compliance**, **scalability** through **customer privacy**, and **fraud prevention**.

Blockchain brings decentralized and transparent infrastructure; AI results in intelligent insights due to the power of automation, and the IoT brings real-time connectivity. Therefore, combined, these technologies represent synergistic ecosystems that will power change in financial services and retransform the traditional banking model, defining new innovations in order to give a new face to the future of finance. However, to fully realize this potential, continuous **research collaboration** and **support from regulators** are required. Of course, what is just now beginning is this journey to absorption of such complex technologies where thousands of possibilities can come forth in reshaping the futures of finance and banking sectors alike.

2.10.1 Recap of Key Points

We shall try to elaborate in this book how **blockchain**, **AI**, and **IoT**, **synergized** together, revolutionize the **finance** and **banking sectors** in the following areas:

1. **Blockchain in Banking**:

   - The potential of blockchain technology to also enable **cross-border payments**, **smart contracts**, **securities trading,** and **asset tokenization** has changed the financial landscape.
   - In banking, blockchain supports the process of **Know Your Customer (KYC)**, **loan management**, and **customer data privacy**, the services offered are **decentralized** and enhanced **security**.

2. **IoT's Role**:

   - IoT devices deliver raw, real-time data that makes better **assessment of risks** and **fraud detection** in finance.
   - Buttressing banking with IoT: **credit scoring**, **real-time monitoring**, and **personalized financial services**.

3. **AI's Impact**:

AI enables **predictive analytics**, helps **automated trading**, and **fraud detection** in finance, settings to enhance efficiency in decision-making.

In banking, artificial intelligence avails **customer personalization**, **risk management**, and **loan processing**, hence enhancing the overall delivery of services.

4. **Case Studies**:

Real-world implementations underscore the disruptive changes that such technologies bring-for example, **AI-powered fraud-detection systems,** and **blockchain-based payment solutions**.

5. **Research Gaps**:

Scalability, **interoperability**, and **regulatory compliance** are some of the open issues that both sectors have in order to reach more extended adoption.

6. **Future Prospects**:

Continued **innovation**, **collaboration**, and **regulatory frameworks** are all steps to unlock how blockchain, AI, and IoT can really change finance and banking.

Better, even more protected, and efficient systems—these are what future **financial services** and **banking operations** will take shape from with the might of all these technologies.

2.11 Conclusion

With this coming together of **blockchain**, **AI**, and **IoT**, **finance** and **banking** have entered a new age to settle down into secured, efficient, and transparent operations. They change the very mechanisms by which financial services are delivered and architecture up to a foundation existing within banks.

Blockchain enables decentralized ways of security, and transparency, among others. Blockchain technology has redefined the concepts of cross-border transactions, asset management, and reporting via its distributed ledgers. Robbed of these middlemen in the transactions, the costs reduce while processing time increases though with much more credibility between parties participating in financial transactions and banking services. Smart contracts have made complex financial agreements formerly held under human oversight—such as derivatives and syndicated loans—easier and automated.

On the flip side, AI quickly becomes the enabler in real-time analytics and predictability. That helps financial institutions and banks to access tremendous amounts of datasets across massive repositories which give them predictive insights, fraud detection, and risk management abilities that were unimaginable even a few years back. With AI at its core, institutions are now capable of providing services as per individual needs while working much faster on changing market conditions and automating vast processes that include loan approvals and credit scoring.

IoT adds an increased layer of real-time connectivity with data from various devices and sensors. This enables financial institutions to track assets, assess their risk, and monitor customer activities in real time. Building on IoT possibilities, it now becomes feasible for real-time credit scoring, dynamic pricing models, and enabled supply chain financing-a means of bettering and enhancing agility in the accuracy of financial decisions.

The synergy of these three technologies is then perfectly complemented by blockchain and AI, as it together multiplies the impact created in their ecosystem. They can provide holistic answers to basic problems the finance and banking sector is looking at: security threats, fraud, processing inefficiencies, and much higher levels of transparency required. Blockchain's immutability paired with AI's intelligent analytics and IoT's real-time data has enabled new business models, including decentralized finance (DeFi) and peer-to-peer lending, that could redefine the entire financial landscape.

With many taking on these technologies in the financial system, they also come with challenges associated with them. Factors such as scalability and interoperability among others, together with problems of compliance issues, represent huge research gaps and need to be addressed. For instance, one of the significant concerns of a blockchain network handling substantial volumes of transactions has been its factor of scalability. Then, interoperability becomes a huge challenge. Ideally, several blockchain systems and traditional banking systems ought to function interactively toward effective cross-border transactions.

This is further compounded by the fact that the legal and regulatory framework is also changing. The financial institutions should, therefore, involve the government regulatory body to develop clear and transparent guidelines observable at the same time as building innovation. For example, smart contracts require entirely new legal interpretations, cryptocurrencies require stronger AML and KYC regulations.

The future for finance and banking sectors, therefore, holds great promise. Continued improvement in such technologies can help us bet on better security and efficiency systems, better experiences for the customer, and more agile financial institutions. In the wake of services by financial institutions going increasingly digital, new business models and opportunities will surface. These innovations will pay off in the system for large institutions, but they will also decentralize financial service delivery, hence making access to banking services that, heretofore had been unattainable to previously underserved populations possible.

It will change finance and banking in ways many thought were pure science fiction, using blockchain, AI, and IoT. These technologies will ensure that institutions innovate faster, cost more competitively, with higher security, and more transparency in financial transactions, but this will only be seen to the forefront if industry leaders, regulators, and developers of technologies work closer together. In this sense, it will be the challenges already on the agenda and the continuous efforts to shift the boundaries of innovation even towards a smarter, safer, and more efficient financial ecosystem for tomorrow, transforming these financing industries. Much is yet to be discovered, but how these sectors might result in the end by the shape of the challenges of today and their preparedness for the innovations of tomorrow will define the next stage of this trip.

References

Aave (2021) Decentralized lending and borrowing platform. https://aave.com/

Accenture (2020) Blockchain for risk management and fraud prevention. https://www.accenture.com/

AlphaPoint (2021) Blockchain solutions for financial transactions. https://www.alphapoint.com/

Bank of England (2020) Blockchain and KYC: enhancing accuracy and integrity. https://www.bankofengland.co.uk/

Bank of New York Mellon (2020) Blockchain innovations for risk management and loan processing. https://www.bnymellon.com/

BIS (2017) Central bank digital currencies. Bank for International Settlements. https://www.bis.org/publ/othp33.htm; Aave (2021) Decentralized lending and borrowing platform. https://aave.com/

Bitfinex (2021) Global trading platform for digital assets. https://www.bitfinex.com/

BitRewards (2021) Blockchain-based loyalty program and fraud prevention. https://bitrewards.network/

Blockpoint (2021) Real-time tracking for loyalty programs. https://blockpoint.io/

Buterin V (2020a) Ethereum 2.0: a next-generation consensus mechanism. https://ethereum.org/en/eth2/

Buterin V (2020b) Ethereum white paper: a next-generation smart contract and decentralized application platform. https://ethereum.org/en/whitepaper/

Capgemini (2020) AI and Blockchain in automated trading. Capgemini website

Capgemini (2021a) The impact of IoT on financial services. https://www.capgemini.com/research/iot-finance/

Capgemini (2021b) Harnessing the synergy of IoT, AI, and blockchain in financial services. https://www.capgemini.com/research/iot-ai-Blockchain-finance/

Capgemini (2021c) AI in finance: transforming investment and trading with algorithms. https://www.capgemini.com/research/ai-finance/

Catalini C, Gans JS (2016) Some simple economics of the blockchain. Commun ACM 59(11):24–25. https://dl.acm.org/doi/10.1145/2998436

Centre Consortium (2021) USD Coin (USDC) – a fully backed stablecoin. https://centre.io/usdc/

Centrifuge (2021) Automated loyalty program management with blockchain. https://centrifuge.io/

Chainlink (2021) Decentralized oracles for real-time data. https://chain.link/

Christidis K, Devetsikiotis, M (2016) Blockchains and smart contracts for the internet of things. IEEE Access 4:2292–2303. https://ieeexplore.ieee.org/document/7472278

Compound (2021) Decentralized lending and borrowing platform. https://compound.finance/

Bloom Credit (2021) Decentralized credit scoring with blockchain. https://bloomcredit.com/

Credit Bank of Moscow (2020) Blockchain for enhanced transparency in loan management. https://www.cbm.ru/

CurioInvest (2021) Blockchain-based investment records and tracking. https://curioinvest.com/

Deloitte (2020) Blockchain for securities trading: Enhancing efficiency and reducing costs. https://www2.deloitte.com/us/en/insights/industry/financial-services/Blockchain-securities.html

Deloitte (2021) Blockchain and data privacy: ensuring security in financial services. https://www2.deloitte.com/

DTCC (2021) DTCC's blockchain initiative for securities settlement and clearing. https://www.dtcc.com/insights/research/2021/blockchain-securities-settlement

dYdX (2021) Decentralized derivatives trading platform. https://dydx.exchange/

Ethereum Foundation (2021a) Ethereum whitepaper. https://ethereum.org/en/whitepaper

Ethereum Foundation (2021b) Introduction to smart contracts. https://ethereum.org/en/developers/docs/smart-contracts/

Everledger (2021) Blockchain-based asset verification and fraud prevention. https://www.everledger.io/

EY (2021) Decentralized Finance (DeFi) and AI integration. EY website

Figure Technologies (2021) Streamlining loan origination and servicing with smart contracts. https://figure.com/

Filecoin (2021) Decentralized data storage network. https://filecoin.io/

Finastra (2021) Blockchain for loan syndication and management. https://www.finastra.com/

Gartner (2019) Top 10 strategic technology trends for 2020. https://www.gartner.com/

Gartner (2021) Emerging technology analysis: Blockchain, IoT, and AI. https://www.gartner.com

GDPR (2018) General data protection regulation. https://gdpr.eu/

Hyperledger (2021) Hyperledger fabric: an introduction. https://www.hyperledger.org/projects/fabric

IBM Research (2021) Ethics in AI: toward explainability and fairness in financial systems. https://www.ibm.com

ID2020 (2018) Digital identity: a vision for the future. https://id2020.org/

Kiva (2021) Kiva protocol: blockchain for regulatory compliance. https://kiva.org/

KPMG (2019) Blockchain and data privacy: challenges and opportunities. https://home.kpmg/; Zhang W, Zhou X, Liu Z (2016) Peer-to-peer lending and its future development. J Financ Peer-to-Peer Lend Future Dev Regul Comp 24(3):278–293. https://www.emerald.com/insight/content/doi/10.1108/JFRC-09-2015-0064/full/html

LoyalCoin (2021) Blockchain-based loyalty points system. https://loyalcoin.io/

McKinsey & Company (2020) AI personalization in finance: building customer-centric services. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/personalization-at-scale

McKinsey & Company (2021) AI in risk management and predictive analytics. McKinsey website

Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org

Narayanan A, Bonneau J, Felten E, Miller A, Narayanan V (2016) Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.

Nexus Mutual (2021) Decentralized insurance solutions. https://nexusmutual.io/

OpenLaw (2021) Blockchain-based smart contracts for derivatives. https://openlaw.io/

People's Bank of China (2021) White paper: Progress of research & development of E-CNY in China. http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584119071.pdf

Polymath (2021) Security token issuance and management platform. https://polymath.network/

Propy (2021) Blockchain for real estate transactions. https://propy.com/; Zhao X, Wang S, Yu W (2018) Initial coin offerings: financing for startups or speculative investments?. Int J Financ Stud 6(4):1–22. https://www.mdpi.com/2227-7390/6/4/80

PwC (2019) Fund administration services: innovations and insights. https://www.pwc.com/

PwC (2020) Blockchain and compliance: improving loan management processes. https://www.pwc.com/Accenture; (2020) Blockchain for risk management and fraud prevention. https://www.accenture.com/

RealT (2021) Tokenized real estate investments. https://realt.co/

Ripple (2020) RippleNet: faster, lower-cost global payments. https://ripple.com/ripplenet

Ripple (2021) How Ripple's blockchain technology is transforming cross-border payments. https://ripple.com/solutions/cross-border-payments/

SelfKey (2021) Decentralized digital identity verification. https://selfkey.org/

SmartContract (2021) Creating secure smart contracts for financial agreements. https://smartcontract.com/

Sovrin Foundation (2021) Decentralized digital identity with Sovrin. https://sovrin.org/

Spring Labs (2021) Blockchain-based solutions for loan processing and credit risk. https://springlabs.com/

Synthetix (2021) Automated trading of synthetic assets with blockchain. https://synthetix.io/

The Open Platform (2021) Decentralized trading and market transparency. https://theopenplatform.io/

Thomas LC (2009) Consumer credit models: pricing, profit and portfolios. Wiley

Token Rewards (2021) Integration of loyalty programs with blockchain. https://tokenrewards.io/

tZERO (2021) Blockchain-based digital securities trading platform. https://tzero.com/

Uniswap (2021) Decentralized cryptocurrency exchange. https://uniswap.org/

Uphold (2021) Blockchain-based financial transactions and smart contracts. https://uphold.com/

We.Trade (2021) Blockchain-based trade finance and syndicated loans. https://we.trade/

Winding Tree (2018) Winding tree: decentralized travel marketplace. https://windingtree.com/

World Bank (2020) Blockchain for improving loan management and credit risk assessment. https://www.worldbank.org/

Yearn.Finance (2021) Decentralized asset management and yield farming. https://yearn.finance/

Zcash (2021) zk-SNARKs: zero-knowledge proofs for privacy. https://z.cash/

Zhang W, Zhou X, Liu Z (2016) Peer-to-peer lending and its future development. J Financ Regul Comp 24(3):278–293. https://www.emerald.com/insight/content/doi/10.1108/JFRC-09-2015-0064/full/html

Zhao X, Wang S, Yu W (2018) Initial coin offerings: financing for startups or speculative investments?. Int J Financ Stud 6(4):1–22. https://www.mdpi.com/2227-7390/6/4/80

Zohar A (2015) Bitcoin: under the hood. s ACM 58(9):104–113. https://dl.acm.org/doi/10.1145/2701418

Chapter 3
Blockchain Application in Smart Cities Cyber-Physical Infrastructures

Priya Khune, Mayuresh Gulame, Komal Munde, Kanchan Wankhade, and Mohini Kumbhar

Abstract Speedy urbanization imposes innovative resolutions to effectively manage assets, infrastructure, and civilian amenities. Smart cities, leveraging interconnected strategies and data collection, offer an auspicious approach. However, security, transparency, and data integrity remain acute challenges in these complex environments. The distributed ledger system and tamper-proof records of blockchain technology make it an encouraging game-changer for smart cities. The transformational potential of blockchain expertise to develop the productivity and safekeeping of smart towns is examined in this chapter. This chapter tackles the security issues that are common in many areas of smart city development, plus supply chain management, health care, transportation, energy, financial organizations, and data center networks. Blockchain is integrated because of its auditability, transparency, immutability, and decentralization. The paper looks at blockchain technology's potential in various smart city domains after giving some background information on the subject. Regulatory organizations generally don't know enough about current infrastructures, which makes blockchain adoption difficult even with its promise. This chapter deliberates on the benefits plus experiments of incorporating blockchain technology into smart city infrastructures and offers suggestions for further research.

P. Khune (✉) · M. Gulame · K. Munde · K. Wankhade · M. Kumbhar
Department of Computer Science, School of Computing, MIT Art, Design and Technology University, Pune, India
e-mail: priyakhune05@gmail.com

M. Gulame
e-mail: mayuresh2103@gmail.com

K. Munde
e-mail: komal.munde@mituniversity.edu.in

K. Wankhade
e-mail: kanchan.wankhade@mituniversity.edu.in

M. Kumbhar
e-mail: mohinikumbhar2021@gmail.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2025

K. Ahmad et al. (eds.), *Fostering Machine Learning and IoT for Blockchain Technology*,
Transactions on Computer Systems and Networks,
https://doi.org/10.1007/978-981-96-4074-4_3

Keywords Blockchain technology · Data management · Management of supply chains · Medical care

3.1 Introduction

For improving sustainability, security, and resource management, this chapter looks at how blockchain technology can be integrated into smart city infrastructures. Sturdy and safe infrastructure is becoming increasingly important as cities around the world experience rapid urbanization and the urban population is predicted to increase dramatically over the next few decades (Alnahari and Ariaratnam 2022). When it comes to providing services with minimal human interaction through data-driven analytics, smart cities leverage a variety of task-oriented tools that are built to nurture urban and environmental demands. Appearing as a potential solution to meet these demands, blockchain is recognized for its efficiency, interdependence, privacy, and transparency. Due to its potential to guarantee privacy, secrecy, and data integrity without physical control, blockchain technology which was first used in Bitcoin has attracted widespread interest.

This research is to investigate how blockchain integration might be implemented in smart cities of the future and how it can tackle the intricate problems of sustainable infrastructure, particularly in light of the anticipated increase in urban population. We go over blockchain's uses in the energy, healthcare, transportation, and governance sectors of smart cities, emphasizing how it can cut out middlemen and improve operational efficiency. Unlike conventional techniques, peers can transfer digital assets to one another without the essential for middlemen cheers to blockchain technology, which was first created for the Bitcoin cryptocurrency. Bitcoin's capital market growth has been phenomenal since its invention by Santoshi Nakamoto in 2008. Through the total elimination of the requirement for a fundamental expert to administer trades, blockchain a decentralized, publicly accessible, and irreversible shared database revolutionized the ways in which nobles mechanize disbursements, communicate, trace, and track trades. The data that smart city devices acquire is typically kept on a chief server for later usage in conventional systems. Several risks can affect these central servers, including the requirement for multiple management authorities at once and the disclosure of private data as a result of unencrypted server data being hacked. For data management and storage, this highlights the necessity of a paradigm change in favor of a decentralized architecture. In this case, blockchain creates a decentralized Peer-to-Peer (P2P) network that allows two devices to trade data, information, and resources. Additionally, blockchain-based systems prevent adversaries from bidding to contact private data or conquest the system as a whole and minimize overall security monitoring costs.

Owing to the extensive use of blockchain technology, several surveys like the ones. Tschorsch et al., for instance, provided an explanation of Bitcoin, its components, and the central mechanism of the Bitcoin protocol. A blockchain-based Journal Pre-proof 4 Internet of Things solution that enables resource sharing in a verifiable way was explained by Christidis et al. Similarly, Kouicem et al. concentrated on the incorporation of blockchain technology and software-defined networking (SDN) in a different study, with an emphasis on the different security requirements for Internet of Things applications. In a different study, Xie et al. examined cutting-edge blockchain technology that enhances smart cities' performance, security, efficiency, and intelligence (Cui et al.).

Despite the fact that blockchain technology and smart cities have been the subject of in-depth research in a number of published literature surveys, the bulk of these studies have focused on these two crucial topics independently. Furthermore, despite its potential, to the best of our information, no prior investigation has thoroughly scrutinized the role of blockchain in achieving security and confidentiality in smart cities. This chapter closes this gap by presenting cutting-edge blockchain technology to address smart city security concerns. The following is an overview of this article's main contributions.

1. Blockchain design and other cutting-edge blockchain skills are offered in this chapter.
2. The investigation of using blockchain expertise to develop smart city performance, safety, and efficiency is the foremost prominence of this work.
3. The usefulness of blockchain across a range of smart communities, including supply chain organizations, economic systems, health care, transportation, and smart grids, is examined in this chapter.
4. The remaining chapter is planned as follows: Blockchain technology's history and architecture are covered in Sect. 3.2. Section 3.3, lists the several characteristics of a smart city. The reasons for implementing blockchain technology in smart cities are explained in Sect. 3.4. The blockchain's current applications to several facets of smart cities are examined in Sect. 3.5. In Sect. 3.6, future study directions are finally selected, and in Sect. 3.7, a conclusion is provided.

3.2 Blockchain: An Overview and Design

Blockchain is an endlessly increasing chain of blocks that stores all dedicated trades in a public ledger. Each deal is cryptographically tested and signed up by all mining nodes. The successive segment will cover the arrangement of blocks, forms of blockchain, compromise procedures, and the undeveloped construction of blockchain technology.

3.2.1 Block Construction

Related to a communal record, a blockchain is an arrangement of blocks that supply transaction data and are linked via reference hashes from previous blocks. The first block, recognized as the beginning block, starts the chain. Each block typically contains a block organization, which consists of trades and a deal counter, and a title, which comprises metadata.

Here are the attributes detailed:

1. **Nonce**: A 4-byte field that twitches from nil and raises for each single hash function. It shows a fundamental role in the proof-of-work algorithm used in mining.
2. **nBits**: A dense illustration of the existing hashing goal. This indicates the difficulty target for the hash and adjusts to ensure the consistent time of block generation.
3. **Timestamps**: The current timestamp. This is used to record the exact time when the block was created.
4. **Merkle derivation tree**: The designed hash of all the trades. It is a single hash derived from all the transactions in the block and helps to efficiently and securely verify the integrity of trades.
5. **Aforementioned block**: A 256-bit hash indicating the prior block. This associates the recent block with the former one, generating a sequence of blocks (blockchain).
6. **Block type**: Recycled to decide the block authentication rule to be followed. This specifies which set of block validation guidelines to monitor.

These attributes collectively guarantee the safety, reliability, and consistency of the blockchain.

In a blockchain system, a deal is often a data structure that represents the transmission of arithmetical possessions among peers. Transactions are spread around the network through the gossip protocol, a flooding-based mechanism. Following successful verification and authentication by miners (peers who mine the blocks at the expense of their computational capacity), a transaction is added to a block (Baheti et al. 2022). Because of the intricate computational riddle that the miners must solve, the miner nodes expend a considerable amount of computer power. The miner who cracks the code the quickest is crowned the leader and gets to make a new block in exchange for a small reward.

Additionally, every other peer verifies the fresh block by means of the agreement mechanism a scheme by which users in a decentralized network originate to a settlement on a particular issue. Following this, the newly formed block is added to the chain, and, with the aid of a cryptographic hash pointer, the subsequent blocks are linked to it. Blockchain uses asymmetric cryptographic techniques like digital signatures to verify the legitimacy of the transaction. A set of encrypted and decrypted keys belongs to each network user. The transaction is encrypted or signed using the private key, but the unrestricted key is broadcast all over the link, visible to all, and used for decryption. In Fig. 3.1, three blocks (Block (n + 1), Block (n), and Block (n − 1) make up the blockchain structure seen in this picture. Every block comprises a header that includes the timestamp, Merkle root, and hash of the preceding block, followed by a body that contains transaction data. The chain's integrity and sequential order are guaranteed since each block is connected by its predecessor's hash.

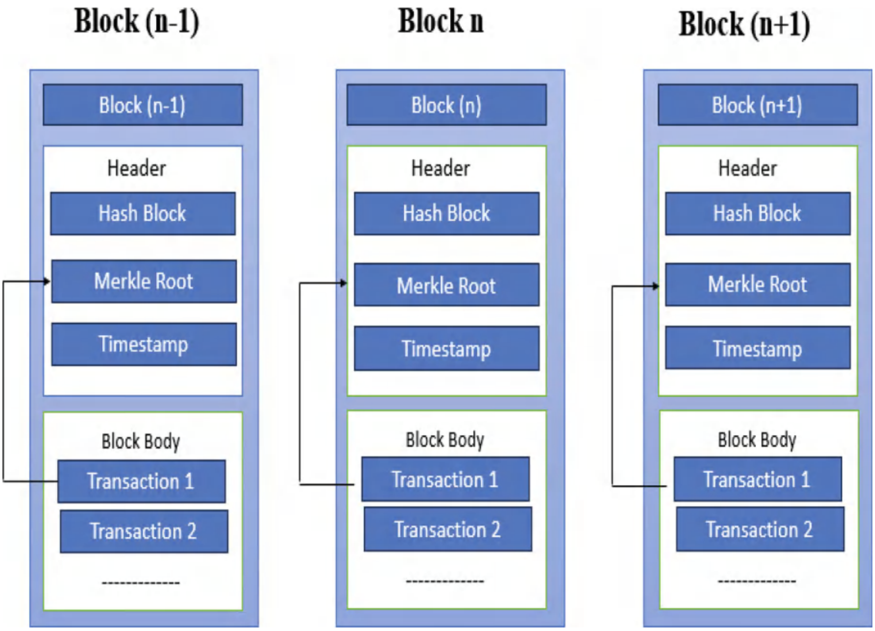


Fig. 3.1 Overall block organization

3.3 Smart City: Features, Pillars, and Safety Necessities

Smart city mentions to the coordinated and planned use of all available resources and technologies to create integrated, sustainable, and livable urban sceneries. The concept of "smart cities" is put to use in many different ways in modern civilizations. These include maximizing energy utilization using smart energy solutions and enabling buildings to control lighting, security, and energy use on their own (smart buildings). In addition, smart technology makes intelligent network connectivity and edge processing solutions possible in metropolitan settings. Intelligent transport system deployment is given priority in smart mobility initiatives. Smart healthcare projects aim to improve general well-being, health monitoring, and diagnostics by utilizing intelligent systems and connected medical devices (Nautiyal et al. 2018). The goal of smart security measures is to reduce security threats in order to protect people, property, and data. Last but not least, smart governance programs seek to make government policies and services available to citizens via digital means. In order to save time and money, a smart city must have a wide range of network connectivity, which raises security concerns. This problem may get worse if IoT devices start gathering data from multiple sources and transferring it to a single location. They raise the likelihood of attacks by giving hackers places to enter the system. By using a variety of techniques, including brute force assaults, SQL injection, eavesdropping, Denial of Service (DoS), and session hijacking, these attackers are able to interfere with intelligent services. To facilitate their operation and ongoing development, smart cities are made up of certain characteristics, themes, and infrastructure. In the sections that follow, we'll go into further detail about these features.

3.3.1 Characteristics of a Smart City

Many features, such as sustainability, intellect, urbanization, and quality-of-life (QoL), are the foundation of a smart city. Urban development's most important paradigm is sustainability, and the upswing of smart towns is a straight outcome of this focus. A few subaspects of sustainability, including social concerns, economics, organization and governance, energy and environment alteration, contamination and waste, and fitness, were suggested by Mohanty et al. The modern world's cities are using natural resources at a much higher rate than ever before, hence it is essential to cautiously consider the effects of depleting non-renewable energy sources. Jong et al. emphasized the necessity of preserving energy sources and natural heritages in demand to ensure the sustainability of smart cities. Sustainability is the capacity of a city to carry out its activities and maintain the ecosystem's balance in each of the aforementioned areas. Increasing a city's total social, economic, and environmental standards is known as "smartness." The economic and emotional well-being of urban citizens indicates an improvement in quality of life (Pourahmad et al. 2018). Urbanization is the term used to describe the political, economic, technological, and infrastructure factors that go into converting a rural area into an urban one. Figure 3.2, illustrates how these subattributes are related to one another and how they are interdependent. The four quadrants of this diagram—smartness, sustainability, urbanization, and quality of life—illustrate the interrelated elements of a smart and sustainable city. Specific variables are linked to each quadrant: for example, smartness is associated with environmental, social, and economic issues; for sustainability, it is linked to governance, infrastructure, and pollution; for urbanization, it is associated with governance, economics, and infrastructure; and quality of life is linked to emotional and financial well-being. The interdependence between these elements is shown by the arrows, which show their cyclical interaction.

When the idea of a "smart city" was first put forth, the objective was to nurture the superiority of lifecycle for the populace by lowering social participation and social learning obstacles through a variety of creative solutions. Present city associations introduce well-defined social policies in order to hire competent citizens to improve the provisions for high-quality city services. As a result, maintaining the financial and emotional well-being of both staffs and societies is vital for QoL enforcement. For example, Chicago launched healthcare service drives to increase the amenities provided to the city's fewer honored citizen groups.

The modern world views smart cities as the next urban utopias. Researchers discovered that smart cities are the ideal answer to the issues brought on by rapid urbanization, including resource shortages, air pollution, transportation jamming, poor human well-being, and waste managing challenges. These elements comprise

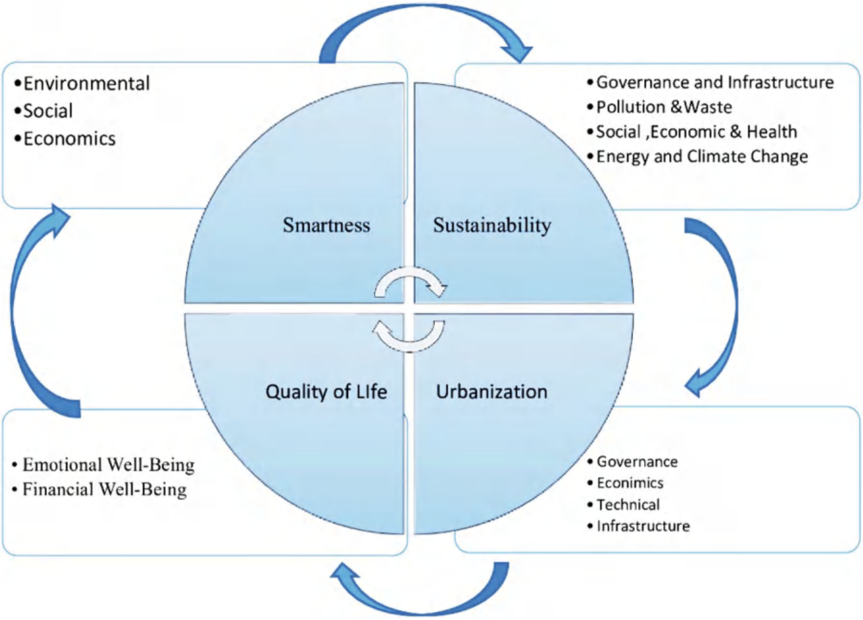


Fig. 3.2 Features of a smart city

the practice of ICT in community organization, ICT approachability, educational attainment, and urban environment awareness. The association concerning urbanization and the rate of carbon emissions in different Chinese towns was examined by Shi and Li (2018).

3.3.2 *Pillars of Smart City*

The four melodies or supports of physical, institutional, social, and economic infrastructure are thought to form the foundation of smart cities. These previously mentioned pillars have the following primary responsibilities.

1. Ensuring resource sustainability and effective city operations are the goals of the physical infrastructure. Together with man-made infrastructure, it is composed of likely resources. The realization of a smart city requires substantial ICT infrastructure and a superior smart object network. The physical infrastructure is expanded to include green constructions, smart energy, building renovations, and green urban planning.
2. The institutional architecture enhances the governance of smart cities through participation in social services, political strategies, translucent governance, and

management. It combines civic, administrative, corporate, and national entities to support the essential service cooperation.

3. Intellectual capital, QoL, and human capital make up the social infrastructure. Social infrastructure plays a vital role in preserving sustainability in smart cities, as the model of smart cities becomes acceptance due to citizen awareness, popularity, and dedication.
4. The commercial structure is the progressive growth of the economy and professions in order to raise municipal throughput by implementing finest practices in e-business and e-commerce.

3.3.3 Security Necessities of Smart Cities

Information and communication technology has affected more or less every phase of our daily life, including personal, educational, and health care as well as national security. Smart city programs were implemented in the majority of government projects to address problems with energy, water, transportation, health, surveillance, and security. Because of their increasing interconnection, complexity, and interdependency, smart cities exclusively make our lives easier but likewise present a variety of security challenges. For the smart city to be implemented safely, a full understanding of these challenges is essential. We look at the main requirements that need to be fulfilled in this section in order to build a safe smart city.

3.3.3.1 Secure Communication

In order to accumulate, share, and move data during a smart city, network communications are essential for connecting the various parts of the architecture. In smart cities, protecting wired and wireless communications requires adherence to the core security principles. It is acceptable to secure communications in smart cities by using lightweight cryptographic algorithms for encryption, decoding, and the generation of shared secret keys.

3.3.3.2 Secure Monitoring and Response

Every system that attempts to detect anonymous behavior and control the environment around it needs to have a monitoring plan. IoT devices that manage data transit and collecting are easy to attacks such the injection of erroneous or misleading device statistics. The organization must take into account elimination or response strategies in order to respond to a questionable activity or an attack. While the reaction plan takes into account a proper occurrence response procedure to counter the vulnerability, the elimination strategy calls for the system to either totally remove or temporarily isolate the impacted IoT device components. Cisco was the company that initially created this type of monitoring response system, which offered suggestions for threat reduction by applying the incident management approach. Nevertheless, the suggested system's applicability is restricted to Cisco network hardware.

3.3.3.3 Secure Booting

Malware such as bugs, worms, and others exist in the form of executable code and can spread over the internet. This aids in their use of boot sectors to overthrow the target structures. Pre-boot malware hijacks the operating system and conceals itself so well that neither virus detection software nor the OS kernel can find it. By preventing the execution of unsigned code in such circumstances, the cryptographic hash-based secure boot technique ensures the integrity and validity of the software packages. Unfortunately, because of their limited computing power, most of the suggested safe booting methods were not suitable for Internet of Things devices. As a result, a very low power consumption hash function based effective boot security solution is suggested for Internet of Things devices.

3.3.3.4 Application Lifecycle Management

IoT devices play a major role in enabling data collecting, analysis, and citizen participation in smart cities. As a result, anticipating the plans and actions required for such devices is essential. Device administration, identity control, software development, and application improvement are all closely tied to the life cycle management of Internet of Things devices. Thus, in addition to taking security precautions into account at each service level, the inventor also needs to verify the key, code, and method elements at each installation and development step. A unique cloud and fog design created data controlling paradigm called Smart-City Comprehensive-Data-Life-Cycle was suggested by Sinaeepourfard et al. with the goal of managing the enormous extents of data gathered during the progress of the lifecycle of smart cities (Kääriäinen and Välimäki 2008).

3.3.3.5 Patching and Updates

IoT devices need software upgrades in order to detect and effectively fix vulnerabilities, which prevents sophisticated security assaults. In addition, an intelligent IoT device is required to verify the authenticity of the patches that are obtained from operators and service providers. To avoid wasting bandwidth, the authentication procedure must not impair the IoT device's functioning, and the safety updates must be available in a downloadable, compact format. A number of IoT devices face difficulties with updating and patching, in addition to being an effective defense against cyberattacks. The primary reason for this is the lack of experience or inexperience of medical equipment manufacturers with dynamic patch updates. Additionally, the limitations imposed make this issue worse.

3.3.3.6 Access Control and Authentication

For IoT systems, managing and controlling the data twisted by the devices while also limiting unwanted access is critical. Unauthorized access must be impossible in smart cities, access by upholding access control, building secure communication, and verifying the identity of the Internet of Things. To protect data privacy in cloud-based smart cities, numerous protocols for authentication and access control have been created. Among these are Attribute-Based Encryption (ABE), Role-Based Access Control (RBAC), and Identity-Based Encryption (IBE). These proprieties help smart cities control who is allowed access and who can be denied it.

3.3.3.7 Application Protection

Identifying system vulnerabilities and ensuring protection against diverse assaults that could be conducted in a smart city typically need the simultaneous application of different methodologies. It is possible to protect IoT device apps using a number of current strategies. To protect the privacy of smartphone applications, for example, smartphones' Unique Device Identifier (UDI), Mobile Equipment IDentifier (MEID), and International Mobile Station Equipment Identity (IMEI) should be secured. Additionally, to safeguard the communication channels and allow safe data transfer between different smart city components, already-existing cryptographic primitives and key management techniques can be used.

3.4 Just Why Blockchain Technology?

The following intrinsic characteristics of blockchain technology make it a compelling answer to the problems listed above with smart cities.

Decentralization:

In a typical centralized system, trustworthiness or endorsement of transactions is derived from central trusted intermediaries. In addition to increasing costs, using a central server reduces overall performance. A centralized third party is not necessary for blockchain technologies to function in a peer-to-peer fashion. With the help of public blockchains, untrusted or unknown nodes can build confidence in a completely decentralized setting. On the other hand, private blockchains function within a closed, trusted environment and use a variety of access control strategies to get the appropriate degree of trust. Permissioned blockchains function similarly to private blockchains in a trustworthy setting, however, they have to maintain data reliability and remove the single point of disaster.

Immutability:

To maintain security, a dependable third party is necessary for any general centralized database, as it is susceptible to hacking. Cryptography ensures the immutability and security of blockchain. Digital signatures are used to sign all transactions, and one-way hash functions that use cryptography are used to securely link the data blocks. This function produces a fixed-length string (referred to as a hash) as output after accepting input of arbitrary length. Because of the shared ledger's immutability, which states that any alteration to one block of data replicates a modification to all of the blocks that follow it, even a minor modification in input causes a major modification in the hash productivity.

Democracy:

Prior to adding a new section to the current blockchain network, all decentralized nodes use consent methods to work together in P2P to achieve a decision. Because all nodes in a blockchain network add to decision-making, the method becomes more democratic.

Security and Transparency:

Since it is difficult to identify one isolated point of error in a blockchain system, the system's total network safety is improved. Additionally, because all transaction records in a blockchain network are publicly accessible, transparency in the system is maintained.

Blockchain technology offers several advantages, including the ability to guarantee data integrity, facilitate open and transparent city management, support collaborative decision-making between individuals and organizations (such as corporations, universities, hospitals, and local and national governments), and facilitate the implementation of democratized smart city initiatives.

3.5 Blockchain Technology for Smart Urban Environments

Smart cities encompass a multitude of elements, including data center networks, supply chain management, smart grid, smart health care, and smart mobility. In each of the aforementioned areas, we examine current blockchain initiatives in this sector. This will provide readers with an enhanced comprehension of blockchain technology's application in relation to smart cities.

3.5.1 Intelligent Health Care

A characteristic healthcare network consists of a collection of clinics under the ownership, management, and sponsorship of a solo organization. However, a single point of error could occur in these centrally managed healthcare networks. In addition, the world's population is becoming more urbanized at a rapid pace, making it difficult for traditional healthcare institutions to meet public demand. A cost-effective, intelligent, and sustainable healthcare system is required in light of the battle between limited resources and the rising request. The most effective way to give healthcare networks the necessary degree of decentralization and consequently increase their security is using blockchain technology.

In Fig. 3.3, a personal healthcare blockchain system is depicted in this diagram, where patient data is securely kept in a decentralized manner from a variety of sources, including wearable technology, biosensors, hospitals, pharmacies, and financial institutions. Data management is done through external storage, guaranteeing patients have access to complete and easily accessible healthcare records.

Wearable technology, emergency response, smart hospitals, and smart ambulance systems are some of the elements that are necessary for the realization of smart health care. Patient data exchange is crucial for an efficient course of therapy since it can enable physicians to assess patients' symptoms in real time, even when they are in remote areas. Blockchain also makes it easier to store medical data securely and irreversibly. Patients can more easily control who has access to their medical records on a flexible basis. Stages that are involved in using blockchain technology to secure healthcare networks. These steps are listed below (Vora et al. 2018).

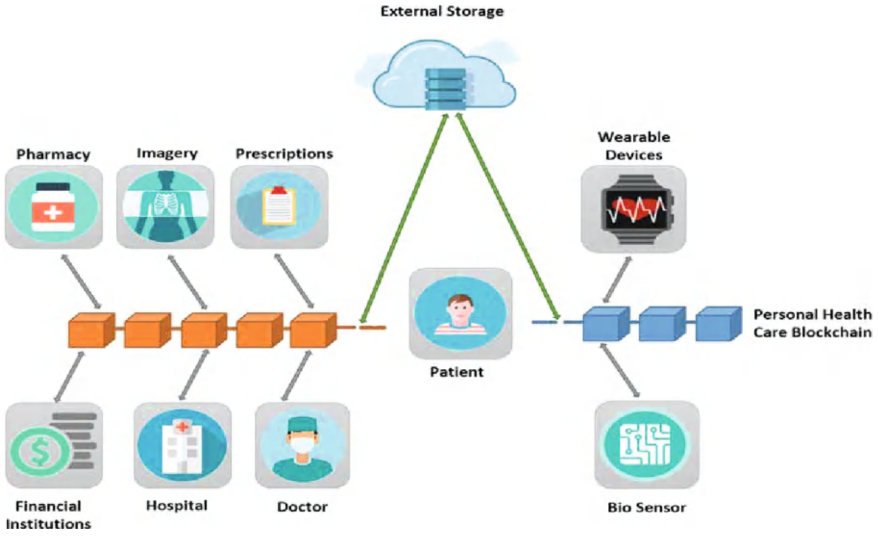


Fig. 3.3 Healthcare network security using blockchain

Step 1: Information about the patient's health, including blood pressure, body temperature, heart rate, respiration rate, blood sugar level, and pulse rate, is collected and tracked by IoT sensors.

Step 2: The administrators create a patient report and keep an eye on the data they have gathered.

Step 3: After reviewing the report, the physicians propose the essential course of action.

Step 4: For extra study, physicians may decide to use a distributed database to exchange the treatment information.

Step 5: The encrypted report that has been verified is distributed.

Step 6: Patients ask to see their treatment record, which is provided by the Cloud Service Provider (CSP).

Step 7: The patient obtains the encoded file comprehending the treatment record when validation is successful.

Step 8: The patients use their own remote key to decrypt the encoded file they expected.

A summary of relevant research on blockchain-based healthcare solutions is provided in the following sections.

3.5.1.1 Best Keeping

Data on medical treatments and digital health records, and patient information are all part of the record management process in a healthcare network.

The work mostly concentrated on research focused on users for medical sectors' public healthcare administration. Based on the data, it appears that blockchain technology can help decentralize healthcare networks.

3.5.1.2 Storage and Exchange of Data

The traditional Sharing of patient medical records across healthcare systems is necessary for healthcare companies that offer services because it is a data-intensive system. Moreover, maintaining the integrity of medical data and keeping it securely in such systems is a difficult undertaking. A WBAN area designated for establishing protected links and a PSN area that uses blockchain technology to share health documents comprised the proposed system. Similar to this, Wang et al. (Wang et al. 2018), suggested a Parallel Healthcare System (PHS) structure for thorough data exchange, maintenance auditability, and examination of health histories. The efficacy of therapy and diagnosis accuracy has been assessed by testing the proposed system on both simulated and real healthcare systems. In Table 3.1, the consensus processes, benefits, drawbacks, and contributions of the various blockchain systems utilized in the healthcare industry are outlined in this table. It stresses concerns such as data security, scalability, and interoperability and encompasses a variety of implementations, including Hyperledger, Ethereum, and Bitcoin. In addition to offering a comparative summary of blockchain applications in health care, each article describes the particular advantages and disadvantages of the suggested solutions.

Table 3.1 A comparative scrutiny of blockchain-based medical resolutions

Reference	Blockchain Platform (consensus used)	Contributions	Advantages	Shortcomings
Ismail et al. (2019)	Bitcoin (PBFT)	Creates demographic clusters from the network users	Minimizes processing overhead and prevents the forking issue	It is still necessary to implement the design in its entirety and assess its performance
Li et al. (2019)	–	Securing mobile healthcare systems' data with the use of edge computing	Effective data commerce and dependable data protection	Does not take data availability and scalability concerns into account
Wang et al. (2018)	Consortium blockchain such as Hyperledger	PHS framework for thorough data exchange and auditability of care	Makes it easier to forecast accurately and provide direction for treating diseases	Susceptibility to problems with scaling and data integrity
Yue et al. (2016)	Ethereum, Bitcoin, Litecoin	DApp to ensure consensus-based, safe, anonymous, and transparent transactions in healthcare systems	Addresses the problems of interoperability and scalability	Does not ensure distant access and data availability
Zhang et al. (2016)	Hyperledger Fabric	The Healthcare Data Gateway (HDG) offers legal and regulatory provisions inside a healthcare system	Ensures that personal medical data is secure and unchangeable	Don't take the consensus algorithm and incentive mechanism into account
Wang et al. (2018)	Ethereum	Included a WBAN section (to create secure links) and a PSN area (to use blockchain for health data exchange)	Ensures safe access to data and identity management	Lacks safe data access and tamper-proof data auditing

3.5.2 Smart Transportation

One of the main causes of the recent surge in interest in smart automobiles has been the advancement of ICT. boosting the effectiveness of travel, and offering convenience to both drivers and passengers are the goals of smart transportation. Blockchain technology can promote information sharing, strengthen system resilience, and enable vehicle communication. Furthermore, blockchain enhances the transportation sector by offering expedited customs clearance, approvals, and document coordination, all while reducing processing times.

3.5.2.1 Vehicular Adhoc NETworks (VANETs)

VANET technology allows automobiles to communicate with roadside units and each other without relying on a central authority. Adversaries may manipulate information in autonomous environments for personal gain. Vehicle authentication is essential for ensuring protected statistics sharing in between automobiles. A number of researchers used blockchain technology to protect message delivery in VANETs. The Merkle Patricia Tree (MPT) is used by the authors to encompass the traditional blockchain construction and enable distributed authentication in the absence of revocation lists. A geographic privacy-preserving blockchain-enabled approach for VANETs created on trust was suggested by Luo et al. In this case, a Dirichlet distribution-based trust managing strategy is developed so that requests and co-operators will only work with vehicles they can trust and the vehicle has access to the associated counterparty trust information since the dependability of the vehicles is documented on a widely accessible chunk.

3.5.2.2 Smart Grid

Fossil fuels, such as coal, natural gas, and oil, provide the majority of the energy used to create power globally. There is a need to employ renewable energy since excessive usage of fossil fuels may raise greenhouse gas emissions and environmental pollution. Due to advancements in battery energy storage technology, consumers are increasingly turning into prosumers who produce and store their own electricity from renewable energy sources. Energy is traded between consumers and service providers through peer-to-peer (P2P) based energy exchange, which is a potent smart grid approach. Many security methods have been put forth to secure the digital transactions that are carried out during this energy trading process while also safeguarding the identities of the customers. A secure, affordable, effective, and sustainable electricity grid system is offered by the smart grid, which is suggested in this regard. Blockchain improves the stability and data safety of these systems in addition to helping to realize a dependable, efficient, and trustworthy decentralized power grid system.

3.5.2.3 Energy Trading

By using blockchain technology and a multi-signature technique, Aitzhan and Svetinovic (2018), presented Priwatt, a decentralized, token-based energy trading system that enables help peers to conduct energy exchange securely and negotiate energy pricing. Gao et al. presented a blockchain-enabled trust-based approach in a different study to foster a trustworthy environment among network users. The goal of the suggested approach is to stop third parties in smart grid networks from manipulating meter readings.

3.5.2.4 Dynamic Pricing

Based on availability and usage patterns, smart grids with dynamic pricing give users flexible and real-time price alternatives. Many dynamic pricing strategies that need the data to pass over an unreliable route have been presented in recent years. In this case, enemies might take over a legitimate organization and update the pricing profiles to harm the smart grid. Blockchain has become a potent tool to ensure a safe and dependable foundation for the online energy industry. The development of an effective microgrid energy framework required the authors to derive seven distinct market components, which include pricing mechanisms, grid connections, information systems, energy management trading systems, regulations, and microgrid configuration. In a similar vein, Agung et al. used blockchain to control transactions and guarantee their immutable execution between producers and consumers. The immutability of the record is maintained by the blockchain, which limits its ability to be altered or removed. Additionally, the suggested approach guarantees that the producer will always supply the consumer with power upon completion of payment. In Table 3.2, various blockchain implementations for energy and smart metering applications are compared in this table, which also highlights the blockchain platforms, contributions, benefits, and drawbacks of each implementation. Data integrity, transaction security, and system scalability are among the problems that are addressed by many solutions, including those that are based on Tendermint, Ethereum, and Bitcoin. Each article describes the particular advantages and drawbacks of the suggested architectures, providing information about their efficacy and areas in need of development.

3.5.2.5 Supply Chain Management (SCM)

A supply chain is a collection of entities, counting businesses and people, who participate directly in the movement of goods, data, and services between a source and its clients. Globally, intricate supply networks have made it possible to produce and market a wide range of goods; nevertheless, the participants in these networks—such as suppliers, retailers, distributors, and carriers—have very little understanding of the lifetime of the items they handle. Nonetheless, this kind of product data is

Table 3.2 Assessment of blockchain based smart grid resolutions

References	Blockchain platform	Contribution	Advantages	Shortcomings
Aggarwal et al. (2018)	Bitcoin, EnergyChain (PoW)	An effective blockchain-secured architecture for storing the data produced by smart meters	Ensures robust auditing, confidentiality, and data integrity	Does not ensure the malleability or immutability of the data
Liu et al. (2019)	Bitcoin	Shamir Secret Sharing (SSS) protocol-based smart metering design	Ensure the legitimacy and accuracy of the data	Does not ensure data audits together with privacy
Rottondi and Verticale (2017)	Ethereum (PoA)	A secluded blockchain to authenticate transactions among EVs	Makes certain that reliable power exchanges between Evs	Does not look into whether the suggested system is scalable
Mengelkamp et al. (2018)	Tendermint	Employs the Brooklyn microgrid structure, which guarantees a suitable ratio between energy production and consumption	Guarantees data reliability and facilitates effective information exchange	The Brooklyn microgrid design in not fully estimated
Agung and Handayani (2020)	Ethereum (Pow)	Used blockchain technology to oversee transactions and guarantee their immutable implementation between users and the creator	The transactions are maintained in their immutability and traceability	Unable to stop individuals from trade electricity produced using cheap or dirty energy
Sheikh et al. (2020)	EnergyChain (PoW)	Framework for consensus that uses a byzantine algorithm to improve data security of DN and EV energy trading operations	Increases system security as a whole and does away with the necessity for any unreliable middleman	Limited physical restrictions on the DN and EVs were assessed by the suggested system

crucial as customers need it to increase their confidence, and industries require it to forecast market trends or make business choices. Consequently, data exchange is a must for the management of supply chains, and it may be accomplished thanks to recent developments in blockchain technology. In addition, blockchain technology may be utilized to track comprehensive product data, stop counterfeit goods from entering the market, and exchange information between different parties to enhance the decision-making process.

A Product Ownership Management System (POMS) that lets the client recognize faked items was proposed by Toyoda et al. The suggested approach uses blockchain technology to effectively track product possession information. Implementing Manufacturers Manager (MM) and Products Manager (PM) smart contracts allows for the realization of "possession of products." While MM keeps track of manufacturer information, PM is in charge of maintaining product position information. Another study by Wu et al. proposed a decentralized, crowd-validated online shipping monitoring system with multiple distributed private ledgers and a single public blockchain ledger.. Sensitive shipment-related data is stored in the private ledger, which also keeps track of custody events. Similar to this, Sharma et al. recommended a distributed method built on blockchain to offer the automobile sector tailored, on-demand, and integrated services.

3.5.2.6 Financial Systems

Money is exchanged between buyers, sellers, customers, and users in a traditional financial system. Thus, protecting consumer privacy and upholding transaction data security rank as the two biggest challenges. In light of this, the best suggested remedy to ensure safe operation management inside an economic scheme is blockchain. The processes involved in a typical blockchain-based financial system's transaction flow are outlined below.

Action 1: Alexa, the customer, sends an application for an agreement to Bank ABC, the supplying bank.

Action 2: The claim letter is sent to the negotiating bank (Bank XYZ) by the issuing bank.

Action 3: Bali (the legatee) receives a letter from the compromised bank urging him to submit the authorization documentation in order to complete the arrangement.

Action 4: Bali sends manuscripts to Bank XYZ.

Action 5: The received document is forwarded to Bank ABC by Bank XYZ.

Action 6: These Manuscripts are made available to Alexa by Bank ABC, who may use them to start a smart agreement with Bali.

Action 7–10: Blockchain facilitates the endangered contract between Alexa and Bali (Fig. 3.4).

A Bitcoin Payment Collection Supervision System (BPCSS) that preserves completely wallet data was proposed by Chen, the transaction information in an economical way to support government agencies on the cloud database, businesses as well as clients (Chen et al. 2017). The suggested framework combines a two-factor authentication system for safe financial transfers, a Quick Response (QR) peer group approach for digital check signing, and a multi-level verification strategy to ensure a secure and impenetrable blockchain-based framework. In order to obtain a well-fitting impact on yield proportion estimates in blockchain economic goods,

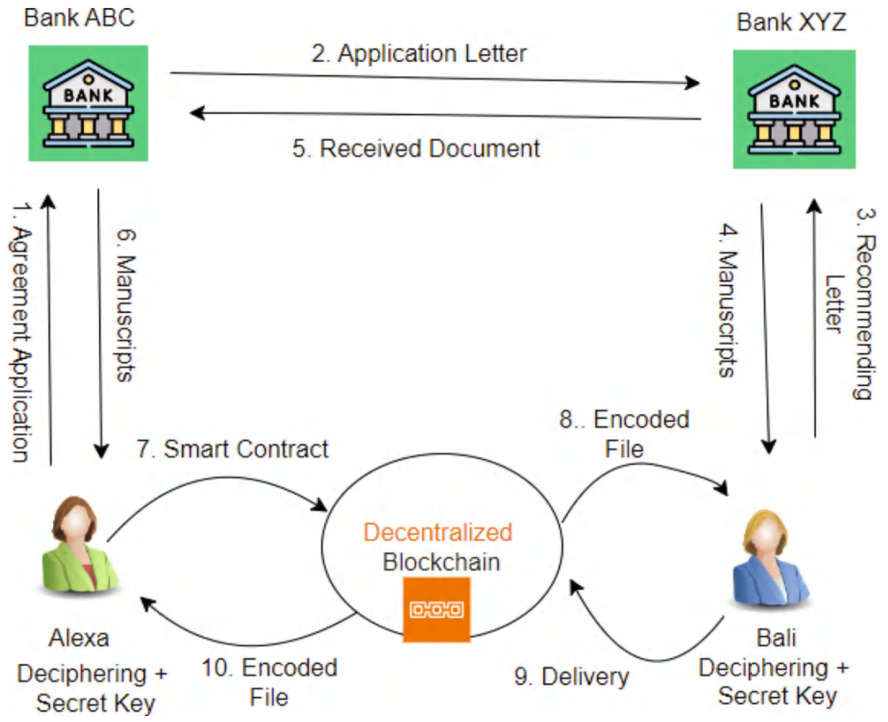


Fig. 3.4 Blockchain in financial systems

the suggested study used back broadcast neural networks, particle swarm optimization (PSO), and support vector regression (SVR) algorithms. The table shows how different studies on blockchain-based financial system solutions compare to one another. The various blockchain-based financial and transaction management systems are enumerated in this table along with information about their platforms, features, benefits, and drawbacks. It highlights their approaches to enhancing data openness, dependability, and transaction security and covers implementations such as Corda, MudraChain, and Bitcoin. Each item highlights the advantages of these solutions—like their immutability and operational flow—while also pointing out their drawbacks, such as their lack of identity management and fraud detection (Table 3.3).

Table 3.3 Blockchain skill for financial use

References	Blockchain platform (consensus used)	Contribution	Advantages	Shortcomings
Khan et al. (2017)	Bitcoin, Corda	A financial agreement management and recording platform called Corda. Hash trees and smart contracts are its foundations	Ensures the financial systems' immutability, dependability, and data transparency	Disregard fraud detection and data availability
Kabra et al. (2020)	MudraChain (PoA)	Combines a two-factor authentication protocol, a QR generating method, and a multi-level authentication scheme	Permits constant clearance operation flow without the need for middlemen	Does not offer clients a actual solution
Chen et al. (2017)	Bitcoin	BPCSS to allow customers and merchandise stores to transact securely. This program is based on Java and Android	Improves affordability, dependability, and transparency	Disregards the need for fraud detection and identity management

3.6 Conclusion

Cities are becoming less sustainable economically and environmentally as an outcome of the world's population explosion and the fast urbanization process. To achieve this, the idea of a "smart city" is put out, which skillfully applies modern ICT to build a justifiable metropolitan environment and increase the quality of life for its residents. However, security issues in smart cities are becoming more and more prevalent. Blockchain's positive qualities (auditability, transparency, immutability, and decentralization) allow it to effectively handle these difficulties. Through a thorough investigation, the latent uses and benefits of blockchain technology in smart cities are discussed in this article, along with some of the drawbacks. The introduction of the report includes some pertinent, newly released reviews and background information on blockchain technology and smart cities. Next, it is explained why blockchain technology is being applied to the field of smart cities. Furthermore, by investigating and evaluating blockchain's application in a variety of smart communities, including supply chain management, health care, transport, smart grids, economic systems, and information center networks, the chapter seeks to bridge the two fields. Lastly, a number of open tasks are listed for potential future research routes in associated fields. The purpose of this chapter is to provide future research on the request of blockchain technology to smart cities with a structured guideline and knowledge base.

References

Aggarwal S, Chaudhary R, Aujla GS, Jindal A, Dua A, Kumar N (2018) EnergyChain. In: Proceedings of the 1st ACM MobiHoc workshop on networking and cybersecurity for smart cities – SmartCitiesSecurity, vol 18. https://doi.org/10.1145/3214701.3214704

Agung AAG, Handayani R (2020) Blockchain for smart grid. J King Saud Univ – Comput Inf Sci 34:666–675. https://doi.org/10.1016/j.jksuci.2020.01.002

Aitzhan NZ, Svetinovic D (2018) Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans Dependable Secur Comput 15(5):840–852. https://doi.org/10.1109/tdsc.2016.2616861

Alnahari MS, Ariaratnam ST (2022) The application of blockchain technology to smart city infrastructure. Smart Cities 5(3):979–993

Baheti S, Anjana PS, Peri S, Simmhan Y (2022) DiPETrans: a framework for distributed parallel execution of transactions of blocks in blockchains. Concurr Comput: Pract Exp 34(10):e6804

Chen P, Jiang B, Wang C (2017) Blockchain-based payment collection supervision system using pervasive bitcoin digital wallet. In: 2017 IEEE 13th international conference on wireless and mobile computing, networking and communications (WiMob). https://doi.org/10.1109/wimob.2017.8115844

Chen PW, Jiang BS, Wang CH (2017) Blockchain-based payment collection supervision system using pervasive Bitcoin digital wallet. In: 2017 IEEE 13th international conference on wireless and mobile computing, networking and communications (WiMob), October 2017. IEEE, pp. 139–146

Cui L, Xie G, Qu Y, Gao L, Yang Y (2018) Security and privacy in smart cities: challenges and opportunities. IEEE Access 6:46134–46145. https://doi.org/10.1109/ACCESS.2018.2853985

Ismail L, Materwala H, Zeadally S (2019) Lightweight blockchain for healthcare. IEEE Access 7:149935–149951. https://doi.org/10.1109/access.2019.2947613

Kääriäinen J, Välimäki A (2008) Impact of application lifecycle management—a case study. In: Enterprise interoperability III: new challenges and industrial approaches. Springer London, pp 55–67

Kabra N, Bhattacharya P, Tanwar S, Tyagi S (2020) MudraChain: blockchain-based framework for automated cheque clearance in financial institutions. Futur Gener Comput Syst 102:574–587. https://doi.org/10.1016/j.future.2019.08.035

Khan C, Lewis A, Rutland E, Wan C, Rutter K, Thompson C (2017) A distributed-ledger consortium model for collaborative innovation. Computer 50(9):29–37. https://doi.org/10.1109/mc.2017.3571057

Li X, Huang X, Li C, Yu R, Shu L (2019) EdgeCare: leveraging edge computing for collaborative data management in mobile healthcare systems. IEEE Access 7:22011–22025. https://doi.org/10.1109/access.2019.2898265

Liu H, Zhang Y, Zheng S, Li Y (2019) Electric vehicle power trading mechanism based on blockchain and smart contract in V2G network. IEEE Access 7:160546–160558. https://doi.org/10.1109/access.2019.2951057

Mengelkamp E, Gärttner J, Rock K, Kessler S, Orsini L, Weinhardt C (2018) Designing microgrid energy markets. Appl Energy 210:870–880. https://doi.org/10.1016/j.apenergy.2017.06.054

Nautiyal L, Malik P, Agarwal A (2018) Cybersecurity system: an essential pillar of smart cities. In: Smart cities: development and governance frameworks, pp 25–50

Pourahmad A, Ziari K, Hataminejad H (2018) Explanation of concept and features of a smart city. Bagh-e Nazar 15(58)

Rottondi C, Verticale G (2017) A privacy-friendly gaming framework in smart electricity and water grids. IEEE Access 5:14221–14233. https://doi.org/10.1109/access.2017.2727552

Sheikh A, Kamuni V, Urooj A, Wagh S, Singh N, Patel D (2020) Secured energy trading using byzantine-based blockchain consensus. IEEE Access 8:8554–8571. https://doi.org/10.1109/access.2019.2963325

Shi X, Li X (2018) Research on three-stage dynamic relationship between carbon emission and urbanization rate in different city groups. Ecol Ind 91:195–202. https://doi.org/10.1016/j.ecolind.2018.03.056

Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Rodrigues JJPC (2018) BHEEM: a blockchain-based framework for securing electronic health records. In: 2018 IEEE globecom workshops (GC Wkshps). https://doi.org/10.1109/glocomw.2018.8644088

Wang S, Wang J, Wang X, Qiu T, Yuan Y, Ouyang L, Guo Y, Wang F-Y (2018) Blockchain powered parallel healthcare systems based on the ACP approach. IEEE Trans Comput Soc Syst 5(4):942–950. https://doi.org/10.1109/tcss.2018.2865526

Yue X, Wang H, Jin D, Li M, Jiang W (2016) Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J Med Syst 40(10). https://doi.org/10.1007/s10916-016-0574-6

Zhang J, Xue N, Huang X (2016) A secure system for pervasive social network-based healthcare. IEEE Access 4:9239–9250. https://doi.org/10.1109/access.2016.2645904

Chapter 4
Towards Secure Healthcare IoT-Opportunities and Challenges of Blockchain

Neetu Sharma and Geetesh Kumar Mishra

Abstract An important step toward improving privacy and security in Internet of Things (IoT) networks is the integration of blockchain technology. This chapter highlights how blockchain technology may improve security and privacy while presenting the fascinating connection between blockchain and IoT devices. The key components of blockchain technology are also discussed such as its robust cryptographic foundation, decentralized architecture, immutable ledger, and smart contract functionality. Additionally, we assessed the degree to which blockchain and IoT are linked to the security of private medical data. This chapter also offers a thorough examination of the challenges and problems that come with integrating blockchain technology into the present healthcare systems. It is necessary to conduct additional research to guarantee scalability, regulatory compliance, and smooth integration of blockchain technology with IoT devices in a secure healthcare setting. This chapter further outlines the limitations and gaps in the existing research as well as potential future directions.

Keywords Cryptography · Data security · Blockchain · Security framework · Privacy framework · Internet of Things · Healthcare

N. Sharma (✉)
Department of Applied Mathematics, Faculty of Technology and Engineering, The Maharaja Sayajirao University of Baroda, Vadodara, Gujarat, India
e-mail: neetus.crypto@gmail.com

G. K. Mishra
Sparklabs Diagnostics India LLP, Vadodara, Gujarat, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2025

K. Ahmad et al. (eds.), *Fostering Machine Learning and IoT for Blockchain Technology*, Transactions on Computer Systems and Networks,
https://doi.org/10.1007/978-981-96-4074-4_4

4.1 Introduction

The growing number of medical patients worldwide is making it harder to access primary healthcare providers. Wearable devices and the Internet of Things (IoT) play a major role in the development of smart cities and Remote Patient Monitoring (RPM). These devices are usually microcontroller-equipped and are simple to wear as accessories or integrate into clothing. Intelligent healthcare systems improve the general public health and lives by encouraging self-sufficiency. These are made possible by wearable healthcare devices that offer vital health information such as blood pressure and glucose levels. However, there are several difficulties still exist, especially concerning resident data storage (Aborokbah et al. 2018; Uprety and Rawat 2020; Sheridan et al. 2022). To increase security of the IoT devices, blockchain technology is being used in the data storage and networking framework of smart healthcare across several cloud providers. Using blockchain technology researchers have ensured data integrity and security within and outside the smart home and enables communication across private network members and authentication. The incorporation of secure IoT devices has resulted in a new age of competent and customized patient services in the rapidly developing healthcare industry (Ahmad and Alsmadi 2021). Although these technological developments have many advantages, they also pose serious difficulties, particularly in terms of patient data security and privacy. Since IoT devices for healthcare become more prevalent protecting the privacy, accuracy, and accessibility of sensitive health data is becoming increasingly important. It has become critical to understand the benefits and drawbacks of blockchain technology in the healthcare industry as it continues to strike a tight balance between innovation and patient welfare protection. This chapter provides detailed considerations on how blockchain technology could change the security and privacy environment of medical IoT devices. Also, this chapter seeks to enhance the ongoing topic regarding blockchain adoption. Diagnoses, treatments, and patient care. Most of the researchers have significantly altered the use of IoT devices in healthcare and smart medical devices however, concerns regarding privacy and security have been brought up by the growing usage of these devices (Al-Hawari and Barham 2019; Kasula 2023). A framework for security and privacy using blockchain technology has emerged as an ideal solution for these problems. In addition, data management and security across multiple businesses might be transformed using blockchain technology. Blockchain technology is mostly recognized for its decentralized and inaccessible characteristics. Blockchain technology also has the potential to enhance data reliability and data exchange while strengthening security for IoT ecosystems. This chapter presents a comprehensive analysis of the outstanding characteristics and capabilities of blockchain technology that make it appropriate for use as a security and privacy framework for the Internet of medical devices. This chapter also addressed the challenges and considerations that should be made while using blockchain in healthcare environments, emphasizing the need for easily integrated, scalable, and compliant solutions. Every component—from decentralization and immutable record-keeping to smart contracts and cryptographic principles is carefully considered with reflection on how it can impact patient information security.

4.2 IoT

The terms "Internet" and "Thing" are combined to form IoT. Anything that can be uniquely recognized is referred to as a "Thing," while the term "Internet" refers to the worldwide network of interconnected computer networks that use standard communication protocols. This implies that any item may have an IP (Internet Protocol) address assigned to it and work in a smart setting, like a medical facility.

The Massachusetts Institute of Technology's (MIT) Auto-ID Center played a major role in popularizing the idea of the "Internet of Things". They started building an RFID (Radio Frequency Identification) infrastructure across companies in 1999. According to a 2002 Forbes Magazine interview, co-founder and previous director of the center Kevin Ashton stated, "We need an internet for things, a standardized way for computers to understand the real world." This piece, entitled "The Internet of Things," was the first to use the phrase in its precise interpretation in writing (Schoenberger 2002). However, in 1999, Neil Gershenfeld of the MIT Media Lab referred to a similar notion in his book "When Things Start to Think (Gershenfeld 1999)," suggesting that the World Wide Web's tremendous development may only be the beginning as more items begin to use the Internet. The term "Internet of Things" has received a lot of popularity in recent years. The first scientific conference on this topic was held in 2008, and by 2005, it began showing up in book titles (Fleisch Mattern 2005; Floerkemeier et al. 2008). In the beginning, European lawmakers mostly discussed the IoT with RFID technology. However, the names of RFID conferences organized by the European Union (EU), such as "From RFID to the Internet of Things" and "RFID: Towards the Internet of Things," suggested a broader strategy (ITU 2005; European Commission 2009). In 2009, the EU Commission finally acknowledged the IoT as a general progression of the Internet, moving from a network of linked computers to a network of connected objects through a specific action plan.

IoT may also mean "global network infrastructure that is dynamic and self-configuring, with standard and interoperable communication protocols." Virtual and physical "things" in this network are seamlessly integrated into the information infrastructure, each with its own distinct identity, physical traits, and virtual features. In simple terms, RFIDs, sensors, actuators, and machine-to-machine communication devices are a few of the cutting-edge Internet technologies that enable the IoT. By way of multiple applications and services, this interconnection offers new business and market opportunities. The following are the key characteristics of IoT technology:

- Utilizing wireless solutions primarily for both indoor and outdoor situations;
- Providing real-time solutions in a worldwide context;

- Encouraging remote environment monitoring and object tracking.

4.2.1 IoT and Healthcare

One of the most important sectors for IoT applications is healthcare. By using the IoT, physicians may help patients virtually, cutting down on the amount of time that separates them. Portable IoT-based health monitoring devices let clinicians assess each patient's health state and customize care. Doctors may remotely monitor patients' health and respond in real-time with the use of portable sensors. Real-time monitoring demands a constant Internet connection, though. IoT is still underused in several medical domains despite its rapid expansion (Sadoughi et al. 2020). There are still certain difficulties in creating appropriate Internet apps for conventional medicine.

In the upcoming years, IoT is probably going to get more attention as medical research keeps expanding. In order to make individualized and well-informed decisions, modern healthcare practitioners must collect, evaluate, and interpret huge amounts of data, which takes time and effort. This procedure may be expedited and simplified using IoT technology. Digital medical data is growing as a result of the extensive use of electronic health records. Examining and evaluating all of this data takes time. Medical personnel also require training on IoT-related technologies (Paranjape et al. 2020; Ergen and Belcastro 2019). Doctors may better personalize therapies to patients' requirements by including IoT and other technologies. They can also handle higher amounts of data and accurately monitor the evolution of diseases.

The IoT brings network-enabled technology, such as portable and wearable devices that can connect and communicate online. Data distribution, consumption, and creation are all changing as a result of this technology. Users commonly utilize these systems to monitor their vital signs, food, sleep, exercise, and other physical ailments, while IoT devices gather and process external information that affects personal health. This interoperability is opening doors for novel therapeutic approaches.. The use of IoT in healthcare is schematically presented in Fig. 4.1.

4.2.2 Applications of IoT in Healthcare

IoT in healthcare has the potential to improve patient management, clinical practice, and research greatly. In a broader sense, it has several uses in the industrial and insurance industries. various four guiding concepts form the foundation of IoT's contribution in multiple domains. The first concept is collecting data, which is facilitated by linked devices like cameras, detectors, monitors, and sensors. The second concept is data conversion, which is the act of converting these devices' analog input into digital form so that it may be processed further. Data storage, which is often handled by cloud-based systems, is the third principle (Bandyopadhyay and Sen 2011; Gopal

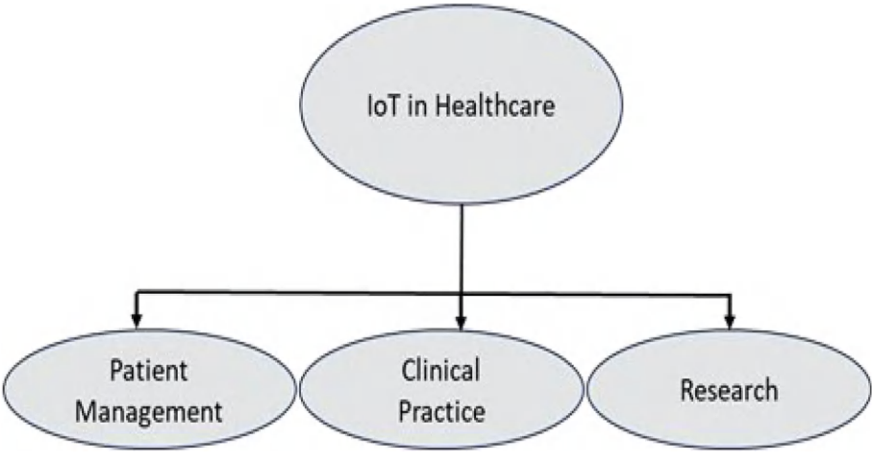


Fig. 4.1 IoT in Healthcare

et al. 2019). Using advanced analytics to process data and provide people with the information they need to make decisions is the fourth principle. Numerous facets of healthcare, such as handwritten patient records and linked laboratory databases, already use these concepts. Wearable technology is the primary element of the IoT infrastructure for patients. These wearables may assess oxygen saturation, blood pressure, pulse/heart rate, and glucose levels according to the required parameters and the patient's medical history. These devices provide tailored treatment for acute and chronic medical conditions. They can also serve as reminders when connected to fitness programs, appointment, and referral systems, or calorie counters. Doctors may immediately reach patients, colleagues, and healthcare facilities with the use of IoT (Mittelstadt 2017). For instance, a cardiologist may receive alerts on a patient's arrhythmia, and a diabetologist may be informed about a patient's hypoglycemia. This makes it possible for patients to get timely medical guidance and support. Doctors can also be able to monitor a patient's adherence to therapy.

Studies indicate that IoT device datasets can help doctors choose the best management and treatment plans for their patients, making a substantial contribution to personalized healthcare. Future research on treatment results may be built using these significant databases. Due to their resources, capacity to handle massive volumes of data, and responsibility for patient care, larger hospitals, and research facilities act as incubators for IoT applications. Apart from overseeing the general health of both inpatients and outpatients, IoT may be utilized by hospitals and laboratories to safeguard equipment like oxygen pumps, wheelchairs, defibrillators, and nebulizers. In order to ensure efficiency and effectiveness, research institutions can also continually monitor experimental activities, equipment deployment, and resource availability. In many situations, multi-dimensional information technology solutions are being created from communication and sensor equipment. Researchers and physicians have been able to create creative healthcare solutions due to emerging IoT methods. IoT-related health research is essential because it can offer high-quality, cost-efficient services and effective preventative treatment. IoT is gradually emerging as a prominent area of study in a variety of academic and corporate domains, most notably medical. As smartphones and wearables become more widely used, IoT approaches are changing healthcare from a conventional, centralized system to one that is more personalized.

To address people's healthcare requirements, e-health has been utilized in a growing way to offer personalized medical services. In the big data age, the IoT is a major advancement since it provides timely technological software solutions for optimizing services (Psiha and Vlamos 2017). IoT data analytics are being used by the medical system today to obtain more data, identify illnesses early, and make vital decisions that will enhance quality of life. The development is being driven by the increasing desire for a better health system. A huge amount of data can be collected, saved, and analyzed because to IoT devices' simultaneous data collection and sharing capabilities with other cloud platforms. These gadgets are helpful for remote environment monitoring and task automation. IoT applications in healthcare have the potential to improve patient outcomes, save costs, and increase access to care. IoT applications may help the insurance business and the healthcare sector. IoT could enhance tasks like data storage, product assessment, medical assessment, and quicker compensation services. However, due to data protection laws and the financial interests involved in handling this information, these applications may encounter serious legal issues (Gupta et al. 2020; Hassija et al. 2019).

A schematic presentation of wearable sensor devices with IoT and blockchain-based secure data encryption in healthcare is shown in Fig. 4.2.

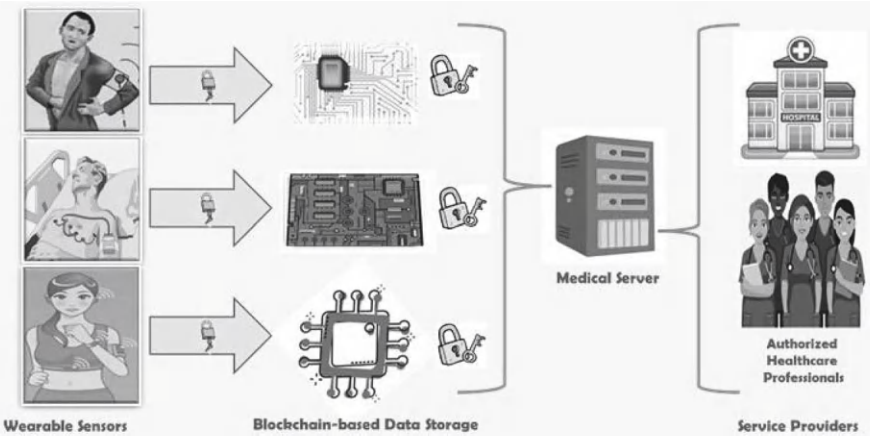

HOSPITAL
Medical Server
Authorized Healthcare Professionals
Wearable Sensors
Blockchain-based Data Storage
Service Providers

Fig. 4.2 Application of IoT in healthcare

4.2.3 Some Benefits of Using IoT in Healthcare

1. Comfort of the Patient: The necessity of frequent hospital visits for emergencies and periodic checks is reduced by remote patient monitoring. To provide proactive care, connected devices store and process data. Early illness identification and prompt medical intervention and therapy are made possible by this method.
2. Low Cost: The cost of at-home care is much lower since patients do not have to go to the hospital for diagnosis or admission, even in an emergency.
3. Accuracy: Information gathered from several sensors (Body Area Network, or BAN) is frequently more accurate than information gleaned from examinations and trips to the hospital. Furthermore, because this data is accurate and is processed often, it can be properly analyzed and has less inaccuracies.
4. Timely therapy: Patients can receive timely and more accurate care before a disease worsens or becomes life-threatening when proactive therapy is facilitated by IoT sensors.
5. Simple management: Sensors gather, store, and process enormous volumes of data. Patients can select which particular information to share with hospital workers using these devices, which handle the data.
6. Automation: Data is sensed, recorded, and analyzed with little to no human interaction. The patient's interaction with technology is improved when all health monitoring and diagnosis procedures are automated.

4.2.4 IoT and Healthcare Architecture

Wearables may gather data from a variety of heterogeneous devices and exchange it with other devices via Bluetooth and Wi-Fi. Big data issues arise from this vast amount of data's volume and pace. In order to ensure that the benefits of this data processing are more than the costs to the healthcare and IoT ecosystem, it must be done so in an effective manner. The architecture outlines the three levels that are required to analyze patient wearable device data to the point of final analysis. The following are these three layers (Al-Fuqaha et al. 2018; Sengupta et al. 2019; Banerjee et al. 2018). Figure 4.3 provides a schematic representation of IoT and healthcare architecture.

4.2.4.1 Device Layer

This layer is in charge of gathering data about the patient, mostly via sensor monitoring, including temperature, blood pressure, peripheral oxygen saturation (SpO2) levels, and other vital indicators. Additionally, it could gather context-aware information about the wearable devices' position or surrounding conditions. The fog layer acts as a bridge in the communication process as the data is sent over a variety of communication protocols to the cloud layer for processing.

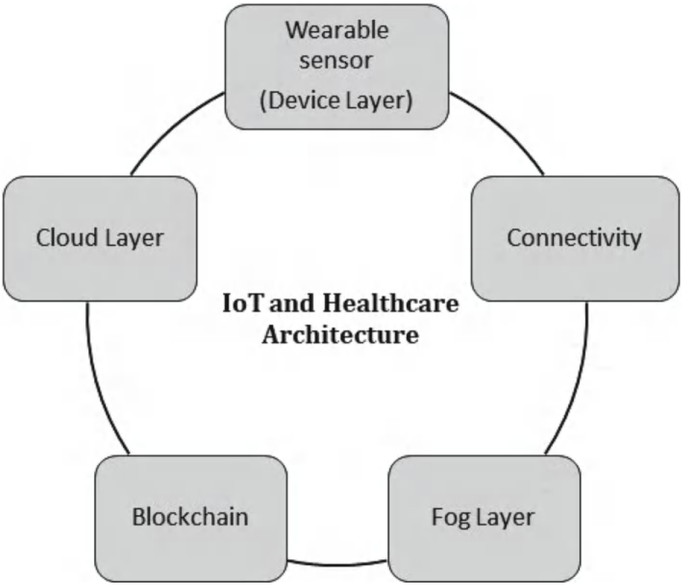

Wearable sensor (Device Layer)
Connectivity
Fog Layer
Blockchain
Cloud Layer
IoT and Healthcare Architecture

Fig. 4.3 IoT and healthcare architecture

4.2.4.2 Fog Layer

Transferring the gathered data from the Device layer to the Cloud layer is the responsibility of this layer. It serves as a channel for the sensed data to go to where it needs to be for analysis. To extract the essential and relevant qualities from the massive volume of data gathered from several heterogeneous devices at the Device layer, preprocessing, filtering, and cleaning the data are required. Furthermore, this layer concentrates on translating one protocol to another for seamless communication because of the diversity of communication protocols and device heterogeneity.

4.2.4.3 Cloud Layer

This layer finally analyzes the data that was supplied by the fog layer, concentrating on information that has been filtered and is important for analysis. To evaluate and predict patients' health, it involves the storage and analysis of data using a variety of machine learning techniques. Significant factors related to patients' health are assessed, guiding physicians and other healthcare providers when recommending treatments.

4.3 Blockchain

Nakamoto (2008) first used the word “Blockchain” to refer to the technology that underpins the virtual currency Bitcoin. With blockchain technology, all transaction records are shared across all nodes in a distributed, peer-to-peer network. Blockchains may be classified into three categories: consortium, private, and public. These are employed to establish connections between different organizations and promote cooperation among the concerned parties. Like private blockchains, consortium blockchains don’t charge for transactions, and they don’t require a lot of processing power to produce new blocks. They still offer auditability and speed up transaction processing, but they fall short of offering total decentralization and censorship resistance (Zheng et al. 2018).

4.3.1 Blockchain Technology in Healthcare

Blockchain technology, which was first made popular by its ability to support cryptocurrencies like Bitcoin, has quickly grown to be an innovative force that has the power to completely change several industries, including healthcare. Blockchain serves as a distributed, decentralized ledger system that records transactions or data in an unalterable, transparent, and safe manner (Polyzos and Fotiou 2017). Blockchain networks propagate data across several participants, each of which gets a copy of the ledger, in contrast to conventional centralized databases, which store data in a single location and are controlled by a single entity. This decentralization guarantees the security, integrity, and transparency of transactions when paired with cryptographic methods. These characteristics make blockchain the perfect answer to the difficult problems of interoperability and healthcare data management. Immutability, decentralization, transparency, security, and smart contracts are some of the key features of blockchain technology that offer enormous potential to transform healthcare administration, delivery, and research. This could ultimately improve patient outcomes and promote innovation in the healthcare industry (Karthikeyyan et al. 2019; Fotiou et al. 2019).

4.3.2 Decentralization Using Blockchain

To improve security, privacy, and general resilience in a Blockchain-based security and Privacy Framework for Healthcare IoT Devices, decentralization is crucial. A central authority becomes obsolete when data is dispersed among a network of nodes in a blockchain system. By preventing a single point of failure, this dispersion lowers the possibility of data breaches and illegal access. Since every node in the network gets a copy of the whole blockchain, fault tolerance and redundancy are improved. A decentralized blockchain architecture distributes patient data among several nodes, contrary to typical healthcare systems that keep it in centralized databases. To eliminate single points of failure and provide redundancy, every node keeps an exact copy of the blockchain. Due to its decentralization, it's very difficult for bad actors to damage the system as a whole by focusing on just one data source. Several nodes participate in the validation of transactions in a decentralized blockchain network (Rahman et al. 2021). Every node has an equal chance to suggest and approve blocks. By distributing validation tasks in a democratic manner the dependency on a single authority is removed, promoting openness and confidence. Decentralized validation also makes the system less susceptible to intrusions or compromised nodes. The security of patient data is significantly improved by blockchain's decentralized structure. A single security breach in a centralized system could compromise the whole dataset. whereas, an attacker would have to take down several nodes at once in a decentralized blockchain architecture, increasing the system's resistance to outside intrusions and cyberattacks. It is the fundamental property that guarantees data added to the blockchain cannot be altered or tampered with by unauthorized parties. Cryptographic hashes are used to link each transaction or interaction with healthcare IoT devices to a block that stores them all. This preserves the integrity of patient health records through the creation of an audit trail that is transparent and verifiable.

4.3.3 Architecture of Blockchain

Data, network, consensus, and application layers are the several levels that make up the blockchain platform. The fundamental data is organized into blocks, each of which is sequentially connected to the blockchain. The network employs the peer-to-peer (P2P) protocol for communication, and distinct consensus processes have been used to achieve consensus. More complex applications may be developed with the help of these fundamental components (Islam et al. 2022). Below are the specifications for each layer.

4.3.3.1 Data Layer

The blockchain is made up of data blocks and a chain structure that functions as a shared data ledger inside a decentralized system. Every data block contains a block address, a block header, and a block body, each of which has a distinct hash value. By storing the hash value of the preceding block, it establishes a link to it, forming a continuous chain. The transaction information is contained in the block body, whereas the hash value, timestamp, and the Merkle tree root value of the preceding block are contained in the block header. The trader digitally signs transactions to guarantee authenticity and guard against manipulation.

4.3.3.2 Network Layer

The network layer manages communication between blockchain nodes. This includes the blockchain network's networking mode and the communication mechanisms between nodes. P2P networking technology, which is decentralized, is used by blockchain. Since each node is equally important and dispersed among different physical places, there isn't a single, centrally located authoritative node.

4.3.3.3 Consensus Layer

The consensus layer includes the relevant consensus algorithms. Common consensus mechanisms are proof of work (PoW), proof of stake (PoS), practical Byzantine fault tolerance (PBFT), and delegated proof of stake (DPoS). PoW is the most widely used consensus mechanism and can tolerate up to 50% of faulty nodes. However, it requires significant hashing power, leading to resource wastage and centralization issues. PoS, on the other hand, avoids these drawbacks by requiring users to hold a stake in the system, making it harder to attack 51% of the nodes. PBFT involves fewer consensus participants, resulting in high efficiency, but its high degree of centralization limits its use in public chains.

4.3.3.4 Application Layer

The application layer encompasses the various use cases of blockchain technology, such as electronic wallets for cryptocurrencies, blockchain applications developed within the Ethereum ecosystem, and other software based on Fabric. This layer offers numerous interfaces for users, allowing them to utilize blockchain technology without needing to understand its underlying mechanisms. As blockchain technology continues to evolve, the range of its application scenarios is expected to expand significantly.

4.4 Related Work of IoT with Blockchain

Numerous studies have mentioned blockchain technology as a potential solution for security and privacy problems with IoT systems. The article explores the various degrees of inherent safety risks associated with IoT devices. In addition, other researchers have looked at more recent solutions for related security flaws and suggest that blockchain technology might be a helpful tool in fixing these problems. In addition, they also look into the concerns related to IoT and industrial IoT (IIoT) and categorize them according to their susceptibility to security breaches. Several authors have also discussed the potential issues that blockchain may have in IoT settings and recommended using blockchain technology to overcome these security challenges. An overview of security issues and associated risks in IoT applications and their solutions has been developed in recent years to improve trust in these systems. Various notable solutions to improve security in IoT devices have been presented in recent years but Four specific solutions i.e. fog computing (FC), edge computing (EC), blockchain, and machine learning (ML) were mostly highlighted as improved security methods in IoT. Among them, Reference (Tandon 2019) has explored IoT security challenges and suggested blockchain as a potential solution. They have also explored the interaction between IoT and blockchain. Further, a smart contract was proposed by Reference (Zhu and Badr 2018) as a solution to security and confidentiality problems in IoT networks. This scheme allows secure communication between IoT devices. They opted for the strategy of decentralized payments, authentication, and access management via blockchain technology. Later, a more exhaustive and efficient approach for resource management in a blockchain-enabled software-defined IoT setup was proposed by Reference (Dorri et al. 2016). This system comprised a distributed flow-rule verification method and an exclusive cluster-head selection mechanism to ensure network security and consistency. In comparison to the conventional blockchain techniques, the suggested blockchain-enabled architecture showed better average throughput, energy consumption, and total end-to-end latency. Additionally, Reference (Hang and Kim 2019) developed a distributed approach that combined Network Function Virtualization (NFV) with Software-Defined Networking (SDN), and blockchain technology for smart city applications. The fundamental concept of this research is an energy-optimized cluster head selection algorithm for effective operations of IoT devices. All the IoT activities are managed by the SDN controller, whereas blockchain technology identifies and prevents cyberattacks in IoT networks. Recently, reference (Kadam and John 2020) evaluated the requirements for developing an identity management system for IoT devices and proposed the integration of blockchain technology with IoT to produce a more effective identity management system that would enhance the reliability and efficacy of the system. More recently, a blockchain-based integrated IoT infrastructure for the safeguarding of sensing data was presented by Reference (Dukkipati et al. 2018). This platform established a technology that might be appropriate for IoT devices with limited resources. In this set-up end users and devices can be monitored and control each other in real-time. Furthermore, Reference (Dorri et al. 2016) recommended the use of Ethereum to solve the issue of power consumption in low-power IoT devices during transaction verification and communication procedures. In this paper, authors have proposed that blockchain may increase the efficacy and efficiency of access control such as blockchain-based access control systems to address security and privacy concerns in IoT platforms. The researchers have also demonstrated how blockchain technology could be utilized to improve IoT security by using it as a decentralized access manager for access control. They also proposed the use of blockchain technology to develop a decentralized control model for IoT systems. This research could enhance the efficiency of access management in IoT solutions. In addition, reference (Zhang et al. 2019) presented an access control method that utilizes several Access Control Contracts (ACCs) using a smart contract system. They also demonstrated the enhancement of the security and privacy of medical data as a cost-effective use case for blockchain technology. Moreover, an electronic health record pseudonym-based encryption system (PBE-DA) was also suggested to enhance the secrecy of medical records. It was evident from various research that blockchain technology can also serve as a link between IoT health devices and medical systems (Badr et al. 2018). Furthermore, Mishra and Tyagi (Mishra and Tyagi 2019) suggested that blockchain technology be used to create an intrusion detection system for the IoT that is capable of analyzing connection behavior and detecting unwanted access. This approach was used in the healthcare sector to safeguard patient data. With a major emphasis on using blockchain in e-health, the research includes statistical data on the papers examined by relevant sectors and the function of blockchain in various IoT solutions. The following part examines the most recent developments in IoT-based healthcare using blockchain technology, as academics' interest in healthcare applications grows. In brief, blockchain technology makes it easier to develop sophisticated management methods for Internet of Things applications. IoT infrastructure may benefit from additional security, trustworthy supply chain management, intelligent manufacturing, remote maintenance, and auditable services due to blockchain technology. A selection of the numerous blockchain-based Internet of Things applications that emerged in recent years includes those related to agriculture (Caro et al. 2018; Leng et al. 2018; Lin et al. 2018), energy (Gai et al. 2019; Gao et al. , 2018), healthcare (Dwivedi et al. 2019; Esposito et al. 2018), industry (Huang et al. 2019; Miller 2018; Mondragon et al. 2018), smart cities (Sharma et al. 2017, 2018; Sharma and Park 2018), smart homes (Dorri et al. 2017; Fernndez-Carams 2015), and transportation (Chen et al. 2018; Lei et al. 2017).

4.5 Security and Privacy of Healthcare Data

Considering the information in healthcare data is highly personal, it is extremely sensitive. Healthcare records, compared to other forms of data, offer comprehensive insights into a person's physical and mental health, medical history, diagnoses, and treatments. If this information is disclosed without authorization, there might be significant consequences, such as discrimination, social stigma, and damage to one's image both personally and professionally. Healthcare data is also often accompanied by financial information concerning insurance coverage, billing, and medical expenses, which makes it an extremely susceptible target for fraud and identity theft. Confidentiality and accuracy of healthcare data are crucial for providing appropriate treatment decisions and medical care thus, strict security measures need to be developed for the protection of patient privacy along with legal and ethical compliance (Aslam et al. 2019). The healthcare sector faces several challenges in ensuring patient security and privacy among them cyberattacks on patient data are becoming more frequent. Additionally, multiple medical devices and digital medical records increase the sources of attack-associated risk of data breaches and unauthorized access. There are also several internal risks associated with employees who have access to sensitive data and may intentionally or accidentally breach security measures. The integration of blockchain technology in the healthcare industry offers both opportunities and difficulties related to security and privacy. In addition to advantages like clear transaction records and safe data storage blockchain technology also poses additional threats like data loss, illegal access, and regulatory non-compliance. Comparably, digital signatures are reported to be used for the improvement of data integrity and authenticity but can also be compromised by illegal usage and key exploitation. To minimize these risks and enhance security in blockchain-based healthcare systems organizations must implement a multi-layered security plan with strong encryption algorithms, and enforced access control to limited authorized users. Also, robust key management protocols should be established to safeguard digital signatures and frequent audits and security assessments must be conducted. Adherence to strict regulatory compliance and defined policies and procedures for data processing, consent management, and incident response should be followed by all the organizations that are involved in data security and IoT device management. Participating in employee training and awareness initiatives may provide staff members with more knowledge of security best practices and the need for patient information protection in blockchain-based healthcare systems (Richter et al. 2019).

4.6 Challenges of IoT in Healthcare

The performance difficulties in healthcare IoT, including technological, financial, security, privacy, and regulatory concerns, provide significant development obstacles. A more advanced system should prioritize optimal security, provide consistent performance, function seamlessly with little power consumption, and encounter minimal delays. An extensive overview of the concerns expressed by several authors on IoT systems in healthcare is given in the next section (Rejeb et al. 2023; Tortorella et al. 2022). A schematic depiction of the challenges brought by IoT in healthcare is shown in Fig. 4.4.

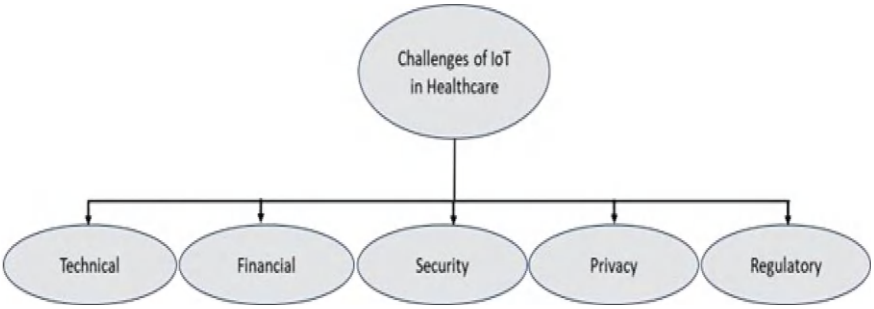


Fig. 4.4 Challenges of IoT in healthcare

4.6.1 Technical Challenges

There are several technological challenges when utilizing IoT in healthcare due to the limited availability of fifth-generation wireless technology in most nations. IoT services have more challenges in becoming broadly accepted in the absence of 5G infrastructure since consumers and healthcare providers often lack awareness of the potential of IoT in everyday life, much alone in healthcare settings. The arrival of 5G technology presents the first major technological obstacle to the deployment of IoT in healthcare. It is costly and time-consuming to deploy more antennae and other 5G equipment. Additionally, concerns about potential health dangers associated with 5G technology have been voiced, despite the lack of sufficient evidence to make clear judgments. Further research is needed to ascertain if widespread use of 5G is safe. It could require a significant amount of time and effort to convince lawmakers that changing public perception is necessary in order to address the global implications of the 5G deployment. However, highlighting the potential benefits of IoT in healthcare might be a compelling argument in favor of investing in 5G infrastructure (Russell 2018).

Bringing together data from several sources is another challenge in technology. The healthcare sector uses a wide range of wearables and data collection instruments, each with its own connection protocol and data format. Manufacturers are still unable to agree on standards, which leads to uneven methods of collecting data. For instance, even when two persons have the same medical condition, they could use various wearables and monitoring equipment to track their vital signs. Delays in data processing might impair decision-making when managing acute illnesses. Moreover, these challenges increase significantly when applied to a large patient population.

4.6.2 Financial Challenges

Regarding the finances, we intend to discuss potential issues with cost-effectiveness. Financially speaking, IoT applications fall under the category of remote health. The budget for remote health monitoring in Europe is now estimated by the International Data Corporation (IDC) to be ∈ 10.41 billion, and it is anticipated to increase by more than ∈ 12.4 billion (Backman et al. 2010). The budget's complexity has thrown off many potential investors, despite its seeming promise for the adoption of IoT in healthcare.

Several factors contribute to financial instability, such as the requirement to work with outside service providers to guarantee the quality of IoT and the necessary infrastructure for connectivity. Without supporting data and historical experience from other healthcare systems or nations, public and commercial healthcare providers have demonstrated a reluctance to engage in the creation of an IoT healthcare network. For background, the IoT healthcare industry was estimated to be worth 60 ∈ billion in 2014 and is expected to grow to 136 billion by 2021 (Li et al. 2019; Reportlinker 2019). IoT in healthcare is predicted to grow at a compound annual growth rate (CAGR) of 12.5% or higher, depending on the ability of healthcare organizations and outsourced providers to reach and sustain a high enough degree of collaboration and understanding. IoT has the potential to ease the financial burden on healthcare if it is put into practice. There are two main types of healthcare costs: direct and indirect. Direct costs are those faced by healthcare providers, whereas indirect costs are those shared by healthcare recipients. Indirect costs include things like missed work, unpaid treatment bills, and family members or other caregivers participating in treatment. Nevertheless, little data is demonstrating the cost-effectiveness of IoT healthcare services because they have not yet been extensively adopted in significant healthcare systems. Economists think that certain aspects of the Internet of Things might lead to a new approach to healthcare development that is less expensive. Among these are efficient product packaging, rigorous quality control, proactive asset management, streamlined inventory, and optimized supply chain management. Even with these established benefits, the ideas have been dominated by industry-focused concepts rather than healthcare-centric ones. To adapt them to clinical practice, economists, healthcare administrators, and physicians will need to work closely together and have a full grasp of each other's perspectives (Allied Market Research 2016).

4.6.3 Security Challenges

Integrating IoT technology in healthcare offers several benefits, including enhanced patient outcomes and real-time patient monitoring. It also raises significant security concerns that must be fixed to protect patient safety and private health information. One major security risk with IoT devices is their susceptibility to hackers. Strengthening security protocols on many IoT and wearable medical devices is extremely difficult because of their limited processing and storage capabilities. As a result, it is opening them up to threats from hackers and viruses. There are significant risks to patient safety with unsecured medical equipment or obtaining unauthorized access to patient health information. Data breaches represent yet another serious issue associated with IoT and medical devices. Personal health information (PHI) is one kind of sensitive data that is frequently captured and exchanged by IoT devices in the healthcare industry. This data could lead to serious privacy violations and financial losses if it is intercepted or accessed by unauthorized individuals. The application of strong encryption methods and safe data storage technologies is necessary to guarantee the security integrity and availability of health data. It is more difficult to implement consistent security measures across various IoT platforms and devices when there are no established security standards. A coordinated approach is necessary for comprehensive protection because there are numerous distinct types of devices each with its own operating system and security features. (Paul et al. 2023).

4.6.4 Privacy Challenges

The massive amount of personal health data generated by IoT devices is one of the main privacy issues. Wearable technology intelligent medical devices and remote monitoring systems gather data on patient's conditions movements and environment constantly. There is a greater chance of abuse and illegal access due to this continuous flow of data. Identity theft and privacy violations could happen if this sensitive information falls into the wrong hands. The challenge of obtaining informed patient consent is another important problem. Patients must understand how Internet of Things devices will gather use and share their data. However, it might be difficult for patients to give their informed consent because IoT systems can be complex and the language can occasionally be long and technical (Bhuiyan 2021). Furthermore, the interconnectivity of IoT devices poses significant privacy risks. Data from a single device may be transferred to multiple platforms and shared with various stakeholders such as insurers outside service providers and medical experts. This vast data exchange increases the likelihood of unauthorized disclosures and data breaches. Data-sharing policies must abide by privacy laws and strict limits on data access must be implemented to lessen these risks. Data anonymization is another matter to be concerned about. Even in situations where patient names have been protected by anonymizing data re-identification is still possible. Advanced data analytics and cross-referencing with other datasets that sometimes permit the re-identification of individuals may jeopardize the privacy of some individuals. Establishing robust anonymization techniques and continuously evaluating and improving them are necessary for the effective protection of patient identities..

4.6.5 Regulatory Challenges

Strict compliance with healthcare laws is necessary to preserve the privacy and confidentiality of patient information. Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) are just two of the strict laws and regulations that protect the privacy of healthcare data. Healthcare organizations can adhere to HIPAA standards for protecting PHI while preserving its integrity, availability, and confidentiality. The handling of personal data about individuals inside the European Union is subject to stringent requirements for data protection accountability and transparency under the GDPR. Due to the wide applications of blockchain technology healthcare organizations now have practical ways to comply with GDPR HIPAA and other pertinent laws. Patient data is stored in an unchangeable decentralized ledger on blockchain which prevents tampering and guarantees data integrity and traceability. Due to its transparency and auditability consent management audit trails and data access restrictions are made possible and could help with compliance. By automating compliance procedures and enforcing predetermined standards programmatic agreements executed on the blockchain or smart contracts can lower errors and administrative burdens. Utilizing blockchain technology and digital signatures in the healthcare sector to adhere to regulations presents certain difficulties despite the possible advantages. Blockchain integration is difficult to implement into the current healthcare systems and procedures and is costly in terms of infrastructure interoperability and training. Furthermore, legal frameworks would not be able to keep up with the rapid advancements in technology which would result in a state of uncertainty and confusion regarding the requirements for adhering to the regulations governing blockchain-based healthcare solutions. Furthermore, it might be difficult to preserve data privacy and protection while making use of the openness and decentralization of blockchain technology since legal requirements might conflict with the transparency and data immutability features of blockchain. Organizations using blockchain-based healthcare systems have to carefully balance the need to protect patient privacy and confidentiality with the need of regulatory compliance. Even if blockchain technology and the Internet of Things have the potential to improve regulatory compliance in the healthcare business, organizations still need to overcome obstacles and restrictions to ensure effective implementation and compliance with regulatory standards (Michele and Furini 2019; Calvillo-Arbizu et al. 2021).

4.7 Future Directions and Conclusion

Massive amounts of data are collected and analyzed by IoT technology, which helps ensure that decisions are made and carried out on schedule. This system is capable of managing such enormous volumes of dynamic data. The widespread adoption of IoT, which ranks among the greatest achievements in human history, is one of the key benefits of the technological revolution. The Internet of Things is becoming more and more popular due to its rapid growth over the last 200 years. It is well recognized that critical decisions need the evaluation of substantial amounts of data related to the processes being considered. It is best to make decisions quickly and use as much real-time data as possible. However, people may not always be able to make prompt and wise decisions. They may bring the medical business several benefits when applied properly. In the modern world, IoT is being adopted by the healthcare industry more and more, which directly affects people's lives and emphasizes the significance of medicine in modern society. Medical systems are one of the most promising disciplines for generating and utilizing large volumes of numerical data. Using IoT technology in the healthcare sector has two main advantages: it may improve patient outcomes and streamline the delivery of healthcare.

It is challenging to turn the vast flow of information into actionable insights without the aid of cutting-edge technologies. Based on empirical data, most healthcare executives anticipate a medical revolution driven by the IoT soon. This revolution is expected to influence three main areas: remote patient health monitoring, preventing exacerbations of chronic illnesses, and data collection. Health is undoubtedly the IoT category growing at the quickest rate. It is anticipated that the number of connected medical devices will increase tenfold during the next ten years. Furthermore, analytics indicate that the quantity of wearable sensors for medical applications will increase significantly over the next two years, from merely 2.4 million units in 2016 to 92.1 million units. At the same time, it's critical to remember that different gadgets and intelligent systems are made to support and optimize the job of medical professionals rather than to take their place of. Using Internet technology, doctors may provide remote care to patients, which is especially important when epidemiological circumstances are getting worse. As a result, IoT makes it possible to provide individualized patient care by enabling customized therapies based on unique medical circumstances. Additionally, IoT can improve medical procedures by automating data collecting in healthcare institutions, increasing medical staff productivity, and facilitating more precise illness diagnosis. This also makes it feasible to track patients' status and the course of their diseases in real time, which improves the standard of treatment even more. IoT also has the potential to increase the efficacy of activities aimed at illness prevention and prediction (Shamila et al. 2019; Pohrmen et al. 2018; Lao et al. 2020; Alam and Benaida 2018; Conoscenti et al. 2016; Risius and Spohrer 2017; Huckle et al. 2016).

By meticulously and effectively combining Blockchain and IoT, medical practice errors may be drastically reduced, which will ultimately enhance patient outcomes. On the other side, the IoT's widespread adoption across several industries caused a lot of discussions. The development of IoT technology is filled with pitfalls and challenges, including a lack of a comprehensive development strategy and an ignorance of its possible uses. These structural barriers need to be overcome if IoT is to fulfill its full potential in the healthcare industry and beyond. The adoption of IoT technology is also fraught with hazards and obstacles that span political, technological, legal, regulatory, educational, financial, economic, security, privacy, and compatibility domains. These obstacles provide several risks when putting IoT ideas into practice, thus further research is required to create all-encompassing solutions for overcoming them. Modern technologies are becoming more and more beneficial in the healthcare industry, as evidenced by the gadgets that continuously monitor health biometrics and timely health-related data. Through the use of mobile applications patients and healthcare providers can now effectively manage their health due to the growing accessibility of smartphones and Internet technologies. The combination of big data and IoT technology is crucial in this context. IoT is changing the way that healthcare is provided by leveraging a platform for seamless communication between different healthcare sectors offering digital support everywhere and enabling modern medicine to progress quickly to satisfy societal demands. By providing accurate information to the right patients at the right time through innovative health systems medical professionals can make timely and efficient medical decisions. Further research is needed to create workable solutions for dealing with these challenges. This chapter offered additional perspectives on the function and uses of IoT technology in the medical field. It has emphasized particular medical situations that show the possibilities and difficulties of implementing an IoT-driven healthcare system in the medical and healthcare field. For the IoT to have a significant impact on healthcare in the future, more research on a range of topics related to its development application and usage is required.

References

Aborokbah M, Al-Mutairi S, Sangaiah AK, Samuel OW (2018) Adaptive context-aware decision computing paradigm for intensive health care delivery in smart cities—a case analysis. Elsevier

Ahmad R, Alsmadi I (2021) Machine learning approaches to IoT security: a systematic literature review. Internet Things 14:100365

Alam T, Benaida M (2018) CICS: cloud-internet communication security framework for the internet of smart devices. Int J Interact Mob Technol 12

Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2018) IoT security: review, blockchain solutions, and open challenges. Future Gener Comput Syst 82(4):395–411

Al-Hawari F, Barham H (2019) A machine learning based help desk system for IT service management. J King Saud Univ - Comput Inf Sci

Allied Market Research (2016) Internet of things healthcare market 2014–2021

Aslam U, Sohail A, Aziz HIT, Vistro M (2019) The importance of preserving the anonymity in healthcare data: a survey. Int J Sci Technol Res 8(11)

Backman W, Bendel D, Rakhit R (2010) The telecardiology revolution: improving the management of cardiac disease in primary care. J R Soc Med 103:442–446

Badr S, Gomaa I, Abd-Elrahman E (2018) Multi-tier blockchain framework for IoT-EHRs systems. Procedia Comput Sci 141:159–166

Bandyopadhyay D, Sen J (2011) Internet of things: applications and challenges in technology and standardization. Wirel Pers Commun 58:49–69

Banerjee M, Lee J, Choo KKR (2018) A blockchain future for internet of things security: a position paper. Digit Commun Netw 4(3):149–160

Bhuiyan MN et al (2021) Internet of things: a review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. IEEE Internet of Things J 10474–10498

Calvillo-Arbizu J, Román-Martínez I, Reina-Tosina J (2021) Internet of things in health: requirements, issues, and gaps. Comput Methods Prog Biomed 208:106231

Caro MP, Ali MS, Vecchio, M., Giaffreda, R.: Blockchain based traceability in agri-food supply chain management: a practical implementation. In: 2018 IoT vertical and topical summit on agriculture-Tuscany (IOT Tuscany), pp 1–4. IEEE (2018)

Chen W, Ma M, Ye Y, Zheng Z, Zhou Y (2018) Iot service based on jointcloud blockchain: the case study of smart traveling. In: 2018 IEEE symposium on service-oriented system engineering (SOSE), pp 216–221

European Commission: Internet of Things – An action plan for Europe. COM 278 (2009)

Conoscenti M, Vetro A, De Martin JC (2016) Blockchain for the internet of things: a systematic literature review. In: Proceedings of the 2016 IEEE/ACS 13th international conference of computer systems and applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016, pp 1–6

Dorri A, Kanhere SS, Jurdak R (2016) Blockchain in internet of things: challenges and solutions; 75. Novo O (2018) Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J 5(2):1184–1195

Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2017) Blockchain for iot security and privacy: the case study of a smart home. In: 2017 IEEE international conference on pervasive computing and communications workshops (PerCom Workshops), pp 618–623

Dukkipati C, Zhang Y, Cheng LC (2018) Decentralized, blockchain based access control framework for the heterogeneous internet of things. In: ABAC 2018—proceedings of the 3rd ACM workshop on attribute-based access control. Co-located with CODASPY 2018, January 2018, pp 61–69

Dwivedi AD, Srivastava G, Dhar S, Singh R (2019) A decentralized privacy-preserving healthcare blockchain for iot. Sensors 19(2):326

Ergen O, Belcastro KD (2019) Ai driven advanced internet of things (Iotx2): the future seems irreversibly connected in medicine. Anatol J Cardiol 22:15–17

Esposito C, Santis AD, Tortora G, Chang H, Choo KR (2018) Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput 5(1):31–37

Fernndez-Carams TM (2015) An intelligent power outlet system for the smart home of the internet of things. Int J Distrib Sens Netw 11(11):214805

Fleisch E, Mattern F (eds) (2005) Das Internet der Dinge. Springer

Floerkemeier C, Langheinrich M, Fleisch E, Mattern F, Sarma SE (eds) (2008) The internet of things. In: First international conference, IOT 2008. LNCS, vol 4952. Springer

Fotiou N, Siris VA, Polyzos GC (2019) Interacting with the internet of things using smart contracts and blockchain technologies. In: Lecture notes in computer science (including subseries lecture notes in artificial intelligence, lecture notes in bioinformatics), LNCS, vol 11342, pp 443–452

Gai K, Wu Y, Zhu L, Qiu M, Shen M (2019) Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Trans Ind Inform

Gao J, Asamoah KO, Sifah EB, Smahi A, Xia Q, Xia H, Zhang X, Dong G (2018) Gridmonitoring: secured sovereign blockchain based monitoring on smart grid. IEEE Access 6:9917–9925

Gao J, Asamoah KO, Sifah EB. Smahi A, Xia Q, Xia H, Zhang X, Dong G (2018) Gridmonitoring: secured sovereign blockchain based monitoring on smart grid. IEEE Access

Gershenfeld N (1999) When things start to think. Henry Holt and Company

Gopal G, Suter-Crazzolara C, Toldo L, Eberhardt W (2019) Digital transformation in healthcare—architectures of present and future information technologies. Clin Chem Lab Med 57:328–335

Gupta S, Malhotra V, Singh SN (2020) Securing IoT-driven remote healthcare data through blockchain. Lect Notes Netw Syst 94:47–56

Hang L, Kim DH (2019) Design and implementation of an integrated IoT blockchain platform for sensing data integrity. Sensors 19(10):2228

Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B (2019) A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access 7:82721–82743

Huang J, Kong L, Chen G, Wu MY, Liu X, Zeng P (2019) Towards secure industrial iot: blockchain system with credit based consensus mechanism. IEEE Trans Ind Inform

Huckle S, Bhattacharya R, White M, Beloff N (2016) Internet of things, blockchain and shared economy applications. Procedia Comput Sci 98:461–466

International Telecommunication Union: The Internet of Things. ITU (2005)

Islam MJ et al (2022) Blockchain-SDN-based energy-aware and distributed secure architecture for IoT in smart cities. IEEE Internet Things J 9(5):3850–3864

Kadam SB, John SK (2020) Blockchain integration with low-power internet of things devices. In: Handbook of research on blockchain technology, pp 183–211

Karthikeyyan P, Velliangiri S, Joseph IT (2019) Review of blockchain based IoT application and its security issues. In: 2019 2nd international conference on intelligent computing, instrumentation and control technologies, ICICICT 2019, July 2019, pp 6–11

Kasula BY (2023) The role of blockchain technology in securing electronic health records. Trans Latest Trends Artif Intell 4(4)

Lao L, Li Z, Hou S, Xiao B, Guo S, Yang Y (2020) A survey of IoT applications in blockchain systems: architecture, consensus, and traffic modeling. ACM Comput Surv 53:18

Lei A, Cruickshank H, Cao Y, Asuquo P, Ogah CPA, Sun Z (2017) Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet Things J 4(6):1832–1843

Leng K, Bi Y, Jing L, Fu HC, Van Nieuwenhuyse I (2018) Research on agricultural supply chain system with double chain architecture based on blockchain technology. Future Gener Comput Syst 86:641–649

Li S, Li M, Xu H, Zhou X (2019) Searchable encryption scheme for personalized privacy in IoT-based big data. Sensors 19

Lin J, Shen Z, Zhang A, Chai Y (2018) Blockchain and iot based food traceability for smart agriculture. In: Proceedings of the 3rd international conference on crowd science and engineering. ACM, p 3

De Michele R, Furini M (2019) Iot healthcare: benefits, issues and challenges. In: Proceedings of the 5th EAI international conference on smart objects and technologies for social good

Miller D (2018) Blockchain and the internet of things in the industrial sector. IT Prof 20(3):15–18

Mishra S, Tyagi AK (2019) Intrusion detection in Internet of Things (IoTs) based applications using blockchain technology. In: Proceedings of the 3rd international conference (I-SMAC) on IoT social, mobile, analytics and cloud, I-SMAC 2019, pp 123–128

Mittelstadt B (2017) Ethics of the health-related internet of things: a narrative review. Ethics Inf Technol 19:157–175

Mondragon AEC, Mondragon CEC, Coronado ES (2018) Exploring the applicability of blockchain technology to enhance manufacturing supply chains in the composite materials industry. In: 2018 IEEE international conference on applied system invention (ICASI), pp 1300–1303

Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. Decent Bus Rev

Paranjape K, Schinkel M, Nanayakkara P (2020) Short keynote paper: mainstreaming personalized healthcare-transforming healthcare through new era of artificial intelligence. IEEE J Biomed Health Inform 1

Paul M, Maglaras L, Ferrag MA, Almomani I (2023) Digitization of healthcare sector: a study on privacy and security concerns. ICT Express 9(4):571–588

Pohrmen FH, Das RK, Khongbuh W, Saha G (2018) Blockchain-based security aspects in Internet of Things network. In: Proceedings of the international conference on advanced informatics for computing research, Shimla, India, 14–15 July 2018. Springer: Singapore, pp 346–357

Polyzos GC, Fotiou N (2017) Blockchain-assisted information distribution for the internet of things. In: Proceedings—2017 IEEE international conference on information reuse and integration, IRI 2017, January 2017, pp 75–78

Psiha MM, Vlamos P (2017) IoT applications with 5G connectivity in medical tourism sector management: third-party service scenarios. Adv Exp Med Biol 989:141–154

Rahman A et al (2021) SmartBlock-SDN: an optimized blockchain SDN framework for resource management in IoT. IEEE Access 9:28361–28376

Rejeb A, Rejeb K, Treiblmaier H, Appolloni A, Alghamdi S, Alhasawi Y, Iranmanesh M (2023) The internet of things in healthcare: taking stock and moving forward. Internet Things 22:100721

Reportlinker (2019) The global internet of things in healthcare market size to grow at a CAGR of 27.6%. Accessed 19 April 2020

Richter G, Borzikowsky C, Lieb W, Schreiber S, Krawczak M, Buyx A (2019) Patient views on research use of clinical data without consent: legal, but also acceptable? Eur J Hum Genet: EJHG 27(6):841–847

Risius M, Spohrer K (2017) A blockchain research framework. Bus Inf Syst Eng 59:385–409

Russell CL (2018) 5G wireless telecommunications expansion: public health and environmental implications. Environ Res 165:484–495

Sadoughi F, Behmanesh A, Sayfouri N (2020) Internet of things in medicine: a systematic mapping study. J Biomed Inform 103:103383

Schoenberger CR (2002) The internet of things. Forbes Magazine, 18 March

Sengupta J, Ruj S, Das Bit S (2019) A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J Netw Comput Appl 149:102481

Shamila M, Vinuthna K, Tyagi AK (2019) A review on several critical issues and challenges in IoT based e-healthcare system. In: 2019 international conference on intelligent computing and control systems (ICCS). IEEE

Sharma PK, Park JH (2018) Blockchain based hybrid network architecture for the smart city. Future Gener Comput Syst 86:650–655

Sharma PK, Moon SY, Park JH (2017) Block-vn: a distributed blockchain based vehicular network architecture in smart city. JIPS 13:184–195

Sharma PK, Rathore S, Park JH (2018) Distarch-scnet: blockchain-based distributed architecture with li-fi communication for a scalable smart city network. IEEE Consum Electron Mag 7(4):55–64

Sheridan D, Harris J, Wear F, Cowell Jr J, Wong E, Yazdinejad A (2022) Web3 challenges and opportunities for the market. arXiv:2209.02446

Tandon A (2019) An empirical analysis of using blockchain technology with internet of things and its application. Int J Innov Technol Explor Eng 8(9 Special Issue 3):1470–1475

Tortorella GL, Fogliatto FS, Espôsto KF, Mac Cawley Vergara A, Vassolo R, Tlapa Mendoza D, Narayanamurthy G (2022) Measuring the effect of healthcare 4.0 implementation on hospitals' performance. Prod Plan Control 33:386–401

Uprety A, Rawat DB (2020) Reinforcement learning for iot security: a comprehensive survey. IEEE Internet Things J 8(11):8693–8706

Zhang Y, Kasahara S, Shen Y, Jiang X, Wan J (2019) Smart contract-based access control for the Internet of Things. IEEE Internet Things J 6(2):1594–1605

Zheng Z, Xie S, Dai HN, Chen X, Wang H (2018) Blockchain challenges and opportunities: a survey. Int J Web Grid Serv 14(4):352–375

Zhu X, Badr Y (2018) Identity management systems for the internet of things: a survey towards blockchain solutions. Sensors 18(12):4215

Chapter 5
A Secured Data Transmission Using Blockchain Technology and Fuzzy Neural Network in e-Healthcare

Sannasi Ganapathy and M. A. Rizvi

Abstract Healthcare applications are widely used by physicians, patients, and the public to update their health status dynamically. Many sensors are used in healthcare applications for collecting input data from end users and it needs to be maintained as sensitive data. The sensitive data needs to be saved safely in network servers. The various attackers are trying to misuse the data. To handle the attackers, people have started using blockchain technology to secure the data effectively by detecting the attackers. This paper proposes a new secured data transmission system called Blockchain Technology that incorporates a Simple Fuzzy Neural Network (BSFNN) using blockchain technology and a simple fuzzy neural network (SFNN) to securely share healthcare data by patients, physicians, and other medical professionals. Here, the blockchain technology incorporates the Caesar Cipher and Elliptic-Curve Cryptography Diffie–Hellman (EC(DH)^2) for securing the data. Moreover, an SFNN is used for detecting the attackers by analyzing the users. The proposed system is tested through experimental results and also proved that the proposed system is superior to other systems with respect to security level, communication time, encryption time, and decryption time.

Keywords Secured data transmission · Neural network · Fuzzy logic · Blockchain technology · Elliptic-curve cryptography · Diffie–Hellman

S. Ganapathy (✉) · M. A. Rizvi
Department of Computer Science and Engineering Education, National Institute of Technical Teachers' Training and Research (NITTTR), Bhopal, Madhya Pradesh, India
e-mail: sganapathy@nitttrbpl.ac.in

M. A. Rizvi
e-mail: marizvi@nitttrbpl.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2025

K. Ahmad et al. (eds.), *Fostering Machine Learning and IoT for Blockchain Technology*, Transactions on Computer Systems and Networks,
https://doi.org/10.1007/978-981-96-4074-4_5

5.1 Introduction

The origin of networking technologies are contributing a lot in the healthcare sector to carry the emerging and sensitive data from one place to another quickly. The cost of spending towards healthcare is reducing drastically with the help of networking technologies (Osario et al. 2019). Recently, the usage of sensors and other digital devices is increased and these are all useful for reducing the disease severity by transferring the current patients or public health data in a short span of time to the physicians. Even though, privacy preservation is necessary for the healthcare sector (Sherstinsky 2020) to maintain secret health data securely on servers. For this purpose, the various security mechanisms that incorporate trust mechanisms, cryptography, routing, intrusion detection systems (IDSs), etc., are available in the literature. However, privacy preservation, data loss, and data misuse are affecting the healthcare sector heavily by losing many people due to a lack of communication about the disease severity level and late treatment as well.

Nowadays, blockchain technology is widely used in various emerging fields including finance. Blockchain technology is categorized into three such as public, private, and consortium blockchains that have their own features. Here, the public blockchain is connected to any computer, which is a part of the Internet. Now, the connected computer is capable of managing the data available in the distributed ledger (Sherstinsky 2020). Next, the blockchain is developed for various businesses by the consortium called semi-private blockchain. Last, the authorized node only can manage the data of the distributed ledger then it is called a private blockchain. Generally, Proof of Stake (PoS), Proof of Authority (PoA), and Proof of Work (PoW) are the three types of consortium mechanisms that can be used by nodes to reach a communal agreement on new blocks to blockchain. To perform mathematical calculations, the PoW is necessary. The blockchain technology development is helpful for storing emerging data securely in decentralized networks.

Generally, blockchain technology is built by using cryptographic algorithms for securing the data that are stored or transferred from one user to another in wireless and distributed networks like the cloud. Here, a block is to be added to the blockchain if it is already available in the market. The data transmissions are carried out with every block that is connected to the block, which came before it on the chain. Because the data is observed and stored in a server with necessary security and integrity. It is a unique tool for the healthcare sector to provide confidence to the patients and the public. Artificial Intelligence (AI) is unavoidable in this world for comfortably passing our daily lives. AI is the base for Machine Learning (ML) and Deep Learning (DL) techniques that are useful for predicting the future by analyzing the current and past data available in the literature. Generally, the ML and DL algorithms are using mathematical and statistical formulae to analyze the data and extract the important features that are helpful for predicting the future in the respective field clearly (Kumar et al. 2022). Recently, the healthcare sector widely used DL techniques rather than ML to monitor the health conditions of the patients who are available remotely through Internet of Things (IoT) technologies. All the gathered health information are formulated as Electronic Health Records (EHR) and stored in a database for analysis.

Blockchain technology and DL techniques are used combinable manner for predicting the future and managing the result safely. This paper proposes a new blockchain-enabled data-sharing model to ensure secured data communication in wireless networks and distributed networks like the cloud. In particular, this model is developed for sharing medical data between patients and physicians or medical professionals. Here, the prediction model incorporates the deep learning algorithm called Long Short-Term Memory (LSTM) for performing an effective prediction process. Moreover, the results are stored or communicated to the concern safely by using blockchain technology. The rest of this chapter is formulated as below: Sect. 5.2 describes the related work by highlighting their contributions, merits, and demerits. Section 5.3 explains the newly developed secured prediction model by providing the necessary formulae. Section 5.4 demonstrates the experimental and comparative results. Section 5.5 concludes the work by highlighting the quantitative achievement of the proposed model with future works.

5.2 Related Work

Many security systems are available in the literature that incorporate the trust mechanism, intrusion detection system, machine learning, and deep learning algorithms for predicting the various kinds of attacks (Banerjee et al. 2018; Clim et al. 2019; Nasurudeen Ahamed and Karthikeyan 2020; Huang et al. 2020; Chen et al. 2021; Srivastava et al. 2021; Saveetha and Maragatham 2022; Pan et al. 2022, 2024; Moudoud and Cherkaoui 2023; Ismail et al. 2024; Yang 2024). Among them, Banerjee et al. (2018) conducted a detailed review of IoT security solutions. They have considered the blockchain technology that facilitates the security of shared datasets in a distributed networking environment. End of their review, they arise nine potential queries that are used to provide protection to the data. Clim et al. (2019) evaluate the usage of blockchain technology to protect healthcare data in mobile healthcare (M-Healthcare) applications. Nasurudeen Ahamed and Karthikeyan (2020) developed a new blockchain technology that incorporated a reinforcement learning algorithm in the process of supply chain management with the incorporation of a heuristic search technique. Their model outperformed the available heuristic searching technique incorporating learning methodology regarding service time and traffic. Huang et al. (2020) developed a new privacy preservation method that uses blockchain technology to maintain the privacy preservation of patients and physicians in distributed network environments. They have done a theoretical analysis and proved privacy preservation by maintaining integrity, security, confidentiality, and availability. Their method outperformed the other privacy preservation methods that are available in the literature.

Chen et al. (2021) developed an intelligent federated system with blockchain technology and a multi-agent system. Their system predicts the attackers by analyzing the behaviors and also protects the data securely through blockchain technology. They have achieved better performance in the prediction and security level as well as other systems. Srivastava et al. (2021) identified the challenges in adopting blockchain technology in e-healthcare by conducting a detailed review and analysis. Saveetha and Maragatham (2022) developed a DL-aware IDS with the incorporation of blockchain technology for all emerging fields. Their model outperformed the standard IDSs with respect to detection accuracy in the process of detecting the various attackers. Pan et al. (2022) designed a novel framework that incorporates blockchain technology and DL algorithms for facilitating the decentralized storage and authentication processes. They have used blockchain technology and Convolutional Neural Network (CNN) to find and detect the attacks after verifying the feasibility. Finally, their framework has proven effectiveness and efficiency that are better than other frameworks available in this direction. Moudoud and Cherkaoui (2023) developed a federated learning framework incorporating blockchain technology and trust. They have used a multi-task federated learning method that leverages blockchain to enhance the throughput. Moreover, it allows the training process using various ML algorithms and reduces the training time. In addition, they proposed a bipartite solution as a scheduling method to share the bandwidth from one device to another in the system. Finally, they have obtained superior performance than the existing federated learning framework.

Pan et al. (2024) developed a new DL framework with blockchain technology to store the key values. Moreover, the proposed framework uses a new data-driven rule-based extraction technique for constructing lightweight video. In addition, their framework offers substantial benefits for performing video construction management. In the end, their framework obtained superior performance and proved to be efficient. Ismail et al. (2024) developed a new integrated security framework by applying ML and blockchain technology. Here, ML is used to detect the attacks, and blockchain technology is used to prevent the attackers. Blockchain technology prevents attackers from using smart contractors for authorization and authentication. The ML uses the gradient boosting algorithm to detect the attackers. Finally, it proved the superiority of their model in terms of accuracy with less training and prediction time.

Yang (2024) introduces a new blockchain technology aware cyber security analysis using smart cloud and fuzzy ML algorithms. Moreover, they have used a fuzzy adversarial Q-Stochastic model for deciding the authorized users by applying rules that are constructed by considering the control policies. In the end, their technique achieved better performance in security level, scalability, and energy efficiency. Barve et al. (2024) developed a new blockchain technology incorporating a Support Vector Machine classifier to transmit the data in a secure manner. In their work, an enhanced elliptic-curve cryptography (ECC) is used to perform encryption on public keys that are useful for improving security. Moreover, the ML model optimizes the security parameters that are necessary for transferring the data in a secure manner. At last, their technique obtains a superior security level than other techniques. All the available works provide secured data-sharing services in various networking environments. Even though users are facing various security issues while sharing their sensitive data with patients and physicians. For this purpose, this work proposes a new LSTM-aware blockchain model for ensuring secured data communications in distributed network environments.

5.3 Proposed Work

A new DL-based secured data transmission system that incorporates blockchain technology is proposed in this work for securing healthcare data during data transmission in a wireless network environment including the distributed network environment. This section explains the proposed secured data transmission system by providing the necessary algorithms and formulae with an explanation. This model consists of seven tasks including smart contract, consensus system, registration facility, authentication, encryption mechanism, ciphering mechanism, EC $(DH)^2$ and classification using SVM.

Registration: First, the consensus mechanism has preserved reliability through proof of work. Here, it selects a node that has the hash value of the previous block. Now, the authenticity of each data transmission process is available in the specific active mode. Second, the smart contract is used to check the authenticity of the contract. Moreover, blockchain technology is used in various fields with smart contracts. The learning process through various algorithms can be included in smart contracts. Third, user authentication is necessary for maintaining the privacy preservation of all the users in the networks. The authentication process is to be performed by doing the registration process properly. Finally, the registered users need to be verified properly to avoid the malicious users' re-entry into the network. To avoid the brute-force attack, the hash values are to be used and safeguard the users' login details.

The steps of the registration process are as below:

Step 1: Send the login credentials to the Blockchain (r &#xF0E0; B). Reg = (ID, L).

Step 2: Blockchain generates a 3 digit random number as a unique number (UN).

Step 3: All the future works of Blockchain is to be maintained confidentially.

B &#xF0E0; Hash = (IDS, LS, UNo) hash.

Step 4: Upload the hash value with a number to Blockchain.

Step 5: The hash value is converted into ciphertext.

Step 6: The concerned node submits the request to Blockchain after completion of the registration process.

Step 7: The authentication process is to be initiated and get a hash value AUTr &#xF0E0; B = (IDS, LS, UNunique).

Step 8: After performing the authentication process, initiate the secured routing process by storing the routing table data on a blockchain.

Step 9: Transfer the routing information into the destination node.

Ciphering: Ciphering the given plain text followed by the successful completion of the registration process. Here, the Caesar Cipher (Cc) (Stallings 2011) is used for the conversion process in which every character of the given plain text is to be relocated into a new location based on some specific constraints. For example, A is converted into B, B is converted to C, and it will be continued up to the last one. The Cc works by using the formula given below:

$$\text{Cc} = (D_n + s) \bmod 26$$

where, D_n—original data and s—shift.

This ciphering is capable of providing the minimum level of security to the sensitive data and emerging data that are stored in the network.

Encryption: Encryption offers the restriction to access the data of individuals from a distributed network environment and protect the same from attackers. Encryption is one type of technique to safeguard sensitive data. This work uses Cc to perform the initial level encryption process effectively and prevent unauthorized access by other users.

EC(DH)^2: The EC(DH)^2 (PrabhuKavin and Ganapathy 2020) is used in this work to protect the data by performing the encryption process. Generally, the public key is used in the ECC method to safeguard the data. Here, a curve is demonstrated and the outcome of this determination is performed by using a method according to the prime numbers to a curve, which has determined vertices. Moreover, the ECC incorporation is a complex task that increases the errors and it affects the throughput. The steps of the EC(DH)^2 are as below:

EC (DH)^2 Algorithm.

Input: User data as plain text with a combination of numbers, alphabets, and symbols.

Output: Plaintext.

Step 1: The user IDs are taken as (a,b) values like curve points.

Step 2: Generate a curve for IDs.

Step 3: G is considered as the key generation point and read the plaintext as “p” with size.

Step 4: Let us assume that A as the data that is chosen, Xd is considered as encrypted data, P1 holds a private key, P2 holds a Public key and K is considered as a variable and it holds 67.

Step 5: Find the value of P2 by performing multiplication using p and P1.

Step 6: Chosen data is encrypted through K and P2 and the result is stored in Xd.

Step 7: Let’s assume that CX holds Ciphertext1 and Yd has decrypted text.

Step 8: CX is taken from encrypted data (ED) by performing the multiplication on K and p.

Step 9: Plain text is extracted from encrypted data by using the formula

$$\text{DD} = \text{ED} - (\text{P1} * \text{CX})$$

where DD represents decrypted data.

Step 10: Perform key generation process by applying $\text{K2} = (\text{nA} \times \text{nB})\ 2 \times \text{G}$.

Step 11: K2 holds Cipher-text.

Step 12: Perform the decryption on K2 by applying nB.

Step 13: Plain text G is derived from ((K2, A2) nB2) + 1

Step 14: Return the plain text.

The input data is securely handled in the distributed network environment during the transmission by using these two algorithms by applying two levels of encryption processes. After completing the registration process and encrypting the data, the user categorization process is necessary to identify the attacker. For this purpose, the existing SFNN is used in this work for identifying and detecting the attackers for avoiding the communication delay and loss.

Classification using Simple Fuzzy Neural Network: The classification is done by applying the Simple Fuzzy Neural Network (SFNN) algorithm. Here, the user classification process is done by using the existing SFNN algorithm.

The steps of the SFNN are given below:

Step 1: Read the input data from blockchain with the necessary details.

Step 2: Identify the less distance Distm node by considering all features.

Step 3:Find F value using the Gaussian Fuzzy membership function by considering the Distmand there is no center

Step 4: Identify the two minimum distanced vectors with the indices of k1 and k2.

If distance <Distm

If (label[k1] == label[k2])

Remove the Gaussian center k2 and reduce the no of Gaussians

Go to Step 4.

Step 5: Read the next user input as x for classification

Step 6: Find the maximum Gaussian centers for the input user × by considering the k1 and k2 values.

Step 7: Categorize all the users of the networking environment and stop the process. If not go to Step 5.

Step 8: Return the classified result.

End of this algorithm, all the users are to be categorized as normal users and the attacker based on the analysis results of the user. Finally, the routing table is to be initiated for transferring the users' data from one place to another in the decentralized networks safely. Here, the routing process is also to be done according to the distance between the nodes in the network environment successfully. The incorporation of users' classification using SFNN is useful for avoiding data loss and detecting malicious users. This process is capable of enhancing the quality of data communications securely in the distributed network environment.:

5.4 Results and Discussion

The proposed work has been implemented by using the Ethereum blockchain network that is designed for incorporating e-healthcare applications. Here, a node (user) is used to transmit the data to another node (user) that is responsible for receiving the data safely. This work analyzes the relationship between the PoW and PoA. The new

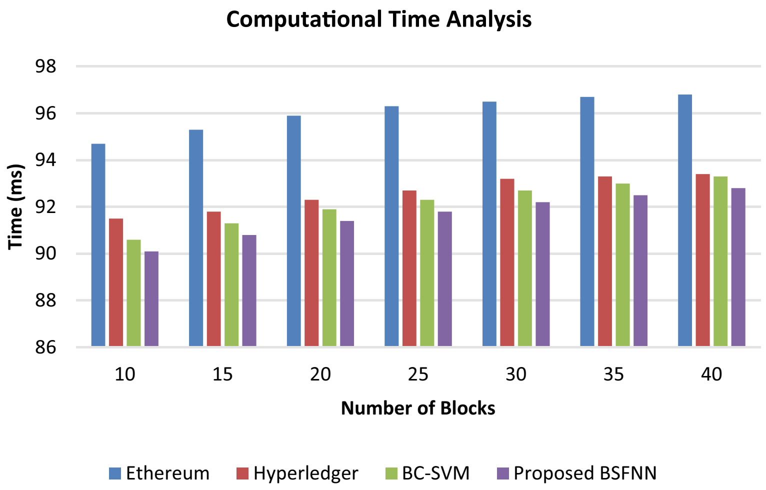


Fig. 5.1 Computational time analysis

system uses a private blockchain where PoA is important. The PoW is necessary for public blockchain to enhance the transaction cost of the transaction along with more computing power. The smart contract is to be executed on blockchain while saving the data of the node. So that increases the transaction cost with respect to the node's volume of records to process in the network. Generally, the time taken is more to transmit the data from one node to another node. This work considers five important evaluation metrics such as security level, computational time, communication time, encryption time, and decryption time to measure the effectiveness of the newly developed system.

Figure 5.1 demonstrates the performance of the blockchain enabled Simple Fuzzy Neural network (BSFNN) with respect to the computational time. Here, six different experiments have been carried out with respect to the number of blocks.

The computational time of the proposed system is lower than the existing security mechanisms including BC-SVM (Barve et al. 2024), Hyperledger (Zhang et al. 2018), and Ethereum (Tariq et al. 2020). This is because of the incorporation of the SFNN and EC(DH)^2.

Figure 5.2 shows the communication time analysis between the newly developed BSFNN and the available blockchain models including BC-SVM (Barve et al. 2024), Hyperledger (Zhang et al. 2018), and Ethereum (Tariq et al. 2020). Here, six different experiments have been carried out with respect to the number of blocks.

The communication time of the proposed system is lower than the existing security mechanisms including BC-SVM (Barve et al. 2024), Hyperledger (Zhang et al. 2018), and Ethereum (Tariq et al. 2020). This is because of the incorporation of the SFNN and EC(DH)^2.

Figure 5.3 shows the encryption time analysis between the proposed BSFNN and available blockchain models including BC-SVM (Barve et al. 2024), Hyperledger

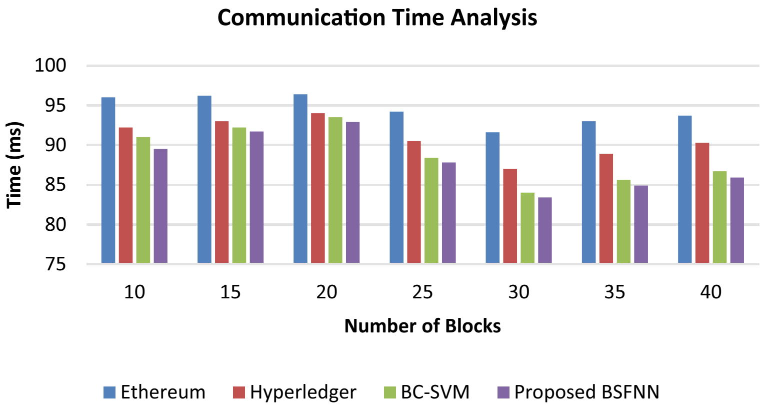


Fig. 5.2 Communication time analysis

(Zhang et al. 2018), and Ethereum (Tariq et al. 2020). Here, six different experiments have been carried out with respect to the number of blocks.

The encryption time of the proposed system is lower than the existing security mechanisms including BC-SVM (Barve et al. 2024), Hyperledger (Zhang et al. 2018), and Ethereum (Tariq et al. 2020). This is because of the incorporation of the SFNN and EC(DH)^2.

Figure 5.4 demonstrates the decryption time analysis between the newly developed BSFNN and the existing blockchain models including BC-SVM (Barve et al. 2024), Hyperledger (Zhang et al. 2018), and Ethereum (Tariq et al. 2020). Here, six different experiments have been carried out with respect to the number of blocks.

The decryption time of the proposed system is lower than the existing security mechanisms including BC-SVM (Barve et al. 2024), Hyperledger (Zhang et al. 2018), and Ethereum (Tariq et al. 2020). This is because of the incorporation of the SFNN and EC(DH)^2.

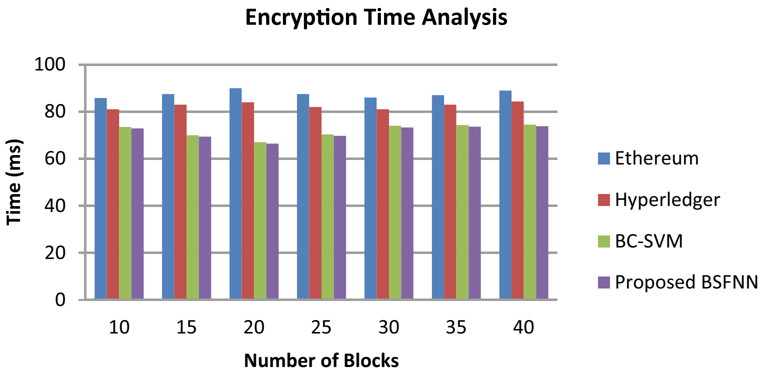


Fig. 5.3 Encryption time analysis

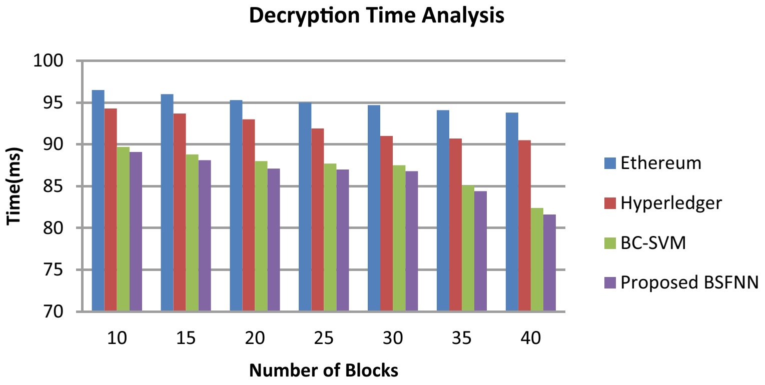


Fig. 5.4 Decryption time analysis

Figure 5.5 shows the security level analysis between the proposed BSFNN and the existing blockchain models including BC-SVM (Barve et al. 2024), Hyperledger (Zhang et al. 2018), and Ethereum (Tariq et al. 2020). Here, six different experiments have been carried out with respect to the number of blocks.

The security level of the newly developed system is lower than the existing security mechanisms including BC-SVM (Barve et al. 2024), Hyperledger (Zhang et al. 2018), and Ethereum (Tariq et al. 2020). This is because of the incorporation of the SFNN and EC(DH)^2.

The proper execution process consumes a certain amount of energy in contrast to Man in the Middle (MITM) attacks and grayhole attacks. To handle these attacks, the routing decision may be changed or diverted to avoid the delay and loss of various applications. The malicious nodes supply a long route and the wrong destination leads to an increase the overall time consumption. Generally, the MITM attack took more time to reach the destination, which is lower time than the grayhole attack. A

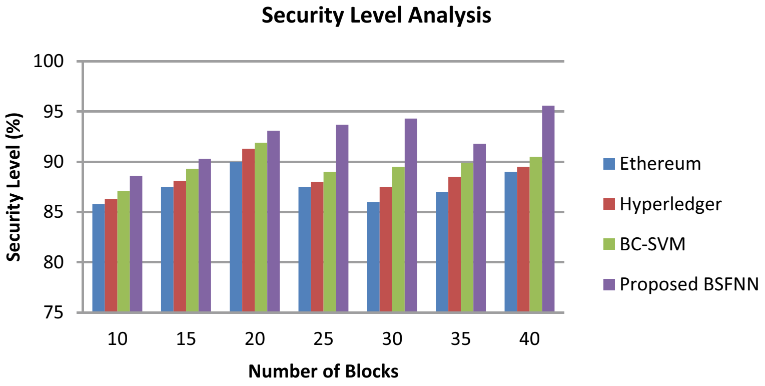


Fig. 5.5 Security level analysis

node needs to contact others repeatedly for transmission when a node is not able to transfer the data to its target location. After detecting the malicious nodes by SFNN, the proposed system consumes less time to find the targeted node's location. So that this secured data transmission system is helpful for maintaining healthcare data securely in a distributed network environment.

5.5 Conclusion

A new secured data transmission system has been developed and implemented in this work with the incorporation of a fuzzy neural classifier and blockchain technology. The authorization process is done by using the Caeser Cipher algorithm. Moreover, the data security is ensured by incorporating the $EC(DH)^2$ and also transferred to the nodes by ensuring user authenticity. In addition, the nodes' genuineness is checked by the SFNN, which recommends the nodes for performing the routing process. However, the proposed BSFNN consumes more time and resources, and a Hyperledger consensus method is also deployed for validating the data transmissions. Finally, the neural classifier is used to find the right destination and the participating nodes that are useful for performing the routing process. This work can be improved further with the introduction of an optimization technique to identify the optimal route which consumes very less time and resources.

References

Banerjee M, Lee J, Choo K-KR (2018) A blockchain future for internet of things security: a position paper. Digit Commun Netw 4(3):149–160

Barve A, Shrivastava M, Saxena AK, Sivaperumal S (2024) Machine learning model on blockchain for secured mobile communication. Meas: Sens 33(101160):1–7

Chen S, Zhang J, Bai Y, Xu P, Gao T, Jiang H, Gao W, Li X (2021) Blockchain enabled intelligence of federated systems (BELIEFS): an attack-tolerant trustable distributed intelligence paradigm. Energy Rep 7:8900–8911

Clim A, Zota RD, Constantinescu R (2019) Data exchanges based on blockchain in m-health applications. Procedia Comput Sci 160:281–288

Huang H, Zhu P, Xiao F, Xiao XS, Huang Q (2020) A blockchain-based scheme for privacy-preserving and secure sharing of medical data. Comput Secur 99(102010):1–13

Ismail S, Nouman M, Dawoud DW, Reza H (2024) Towards a lightweight security framework using blockchain and machine learning. Blockchain: Res Appl 5(1):1–13

Kumar P, Kumar R, Gupta GP, Tripathi R (2022) RDEdge: blockchain and deep learning for secure edge –envisioned green CAVs. IEEE Trans Green Commun Netw 6(3):1330–1339

Moudoud H, Cherkaoui S (2023) Multi-tasking federated learning meets blockchain to foster trust and security in the metaverse. Ad Hoc Netw 150(103264):1–12

Nasurudeen Ahamed N, Karthikeyan P (2020) A reinforcement learning integrated in heuristic search method for self-driving vehicle using blockchain in supply chain management. Int J Intell Netw 1:92–101

Osario DP, Sanchez JD, Alves H (2019) Physical-layer security for 5G and beyond. In: Wiley 5G ref: the essential 5G reference online, December 2019, pp 1–19

Pan X, Zhong B, Sheng D, Yuan X, Wang Y (2022) Blockchain and deep learning technologies for construction equipment security information management. Autom Constr 136(104186):1–11

Pan X, Shen L, Zhong B, Sheng D, Huang F, Yang L (2024) Novel blockchain deep learning framework to ensure video security and lightweight storage for construction safety management. Adv Eng Inform 59(102334):1–12

PrabhuKavin B, Ganapathy S (2020) EC(DH)2: an effective secured data storage mechanism for cloud based IoT applications using elliptic curve and Diffie-Hellman. Int J Internet Technol Secur Trans 10(5):601–617

Saveetha D, Maragatham G (2022) Design of Blockchain enabled intrusion detection model for detecting security attacks using deep learning. Pattern Recogn Lett 153:24–28

Sherstinsky A (2020) Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network. Phys Nonlinear Phenom 404:132306–132349

Srivastava V, Mahara T, Yadav P (2021) An analysis of the ethical challenges of blockchain-enabled E-healthcare applications in 6G networks. Int J Cogn Comput Eng 2:171–179

Stallings W (2011) Cryptography and network security principles and practice, Fifth edn. Pearson Education

Tariq N, Qamar A, Aim M, Khan FA (2020) Blockchain and smart healthcare security: a survey. Procedia Comput Sci 175:615–620

Yang P (2024) Electric vehicle based smart cloud model cyber security analysis using fuzzy machine learning with blockchain technique. Comput Electr Eng 115(109111):1–16

Zhang P, Hite J, Schmidt DC, Lenz G, Rosenbloom ST (2018) FHIRChain:applying blockchain to securely and scalably share clinical data. Struct Biotechnol J 16:267–278

Chapter 6
Secure and Intelligent Patient Monitoring System: Integrating IoT and Blockchain for Real-Time Healthcare

C. Manimegalai, K. Swetha, and R. Thenmozhi

Abstract The blend of blockchain technology and the Internet of Things (IoT) has created an innovative space to look for potential solutions. This paper investigates a Secure and Intelligent Patient Monitoring System (SIPMS) for real-time healthcare using blockchain and IoT technology. In addition, the system is concerned with patient privacy and data security and whether delivering healthcare via this method would be effective—safe and real-time health solutions for patient monitoring systems using blockchain with Internet of Things technologies. The recommended system collects data all the time from patients, hence when needed medical intervention can be done promptly and monitoring is in real time. Blockchain transactions can be put on the decentralized ledger and recorded into a permanent data stream that is unchangeable and secure guaranteeing no risk of information getting exposed to fraudulent intimidation. These technologies create an intelligent decentralized platform, improving the efficiency of healthcare delivery and providing high levels of security. The system aims to revolutionize patient monitoring by ensuring that health data is handled reliably and securely, resulting, ultimately, in better outcomes for patients as well as more efficient medical care. This collects the sensor data using an Arduino and transfers it to the blockchain where, later on, its further viewing after processing. The information produced by machine learning should be fed back to the specialist or caretaker, who then can receive a mail or text. If a critical alert is registered, the specialist/caretaker will then get an SMS and Email notification.

Keywords Electronic Health Records (EHR) · Health data analytics · Decentralized health records · Interoperable health systems · Patient data encryption · Digital health transformation · Secure data sharing

C. Manimegalai
Faculty of Computer Science and Engineering, IFET College of Engineering, Villupuram, India

K. Swetha (✉) · R. Thenmozhi
Department of Computer Science and Engineering, IFET College of Engineering, Villupuram, India
e-mail: swethapk2004@gmail.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2025

K. Ahmad et al. (eds.), *Fostering Machine Learning and IoT for Blockchain Technology*, Transactions on Computer Systems and Networks,
https://doi.org/10.1007/978-981-96-4074-4_6

6.1 Introduction

The approach of progressed innovations has changed different segments, including healthcare. One of the foremost noteworthy advancements is the integration of the Web of Things (IoT) and blockchain innovation into healthcare frameworks, especially in quiet checking. The objective of this integration is to make strides in understanding care's viability, security, and real-time capabilities. Conventional healthcare frameworks confront challenges when it comes to creating a secure and brilliantly understanding checking framework that combines IoT and blockchain.

Interconnected gadgets are utilized to gather, transmit, and analyze persistent information in healthcare. These gadgets, such as wearable sensors and inaccessible checking instruments, permit persistent and real-time following of crucial signs, physical movement, and other well-being measurements. A wearable gadget can send a patient's heart rate to healthcare suppliers in genuine time, permitting for quick reaction to any abnormalities. Convenient therapeutic mediations are progressed by this real-time information collection and examination (Gubbi et al. 2013).

The usage of IoT in healthcare isn't without its challenges, however. One of the most concerns is the security and security of quiet information. Touchy well-being data created by IoT gadgets must be secured from unauthorized get to and breaches. Cyber-attacks can lead to noteworthy protection infringement and monetary misfortunes for conventional information capacity and administration frameworks (Sicari et al. 2015).

These security concerns can be fathomed with blockchain innovation. Blockchain could be a disseminated record that records exchanges over different computers in a way that guarantees the keenness and security of the information. Blockchain innovation can be utilized to defend persistent data, guaranteeing that as it were authorized parties have gotten to it. Each exchange or information passage on the blockchain is scrambled and connected to the past one, making it essentially tamper-proof (Zhang et al. 2018). When a patient's well-being information is overhauled, the blockchain guarantees that it is secure and cannot be changed without discovery.

Moreover, the conveyed nature of the blockchain disposes of the requirement for a central specialist, minimizing the chance of a single point of disappointment. Understanding information is accessible and secure indeed on the off chance that there's a framework breach or disappointment. Blockchain innovation also encourages open and traceable information trades between healthcare suppliers, patients, and other partners, upgrading participation and certainty inside the healthcare environment (Kuo et al. 2017).

Information exactness and unwavering quality are too upgraded by the integration of IoT and blockchain into quiet observing frameworks. Information collected by IoT gadgets is confirmed and recorded on the blockchain. The probability of mistakes and moving forward, by and large, healthcare results are diminished by this real-time information approval (Dwivedi et al. 2019). Healthcare suppliers have precise data for determination and treatment since a blockchain-based framework can confirm the realness of a patient's therapeutic history.

The secure and brilliantly understanding observing framework that combines IoT and blockchain innovation addresses the vital issues of information assurance, protection, and real-time healthcare reconnaissance. Way better well-being results and persistent fulfillment can be accomplished by leveraging these innovations. The progressions within the Web of Things and blockchain will proceed to drive development in healthcare, clearing the way for a future where innovation and pharmaceuticals are consistently coordinated for ideal persistent care.

6.2 Aim of Study

A blockchain-enabled, secure, and shrewdly quiet checking framework will make strides in real-time healthcare conveyance, concurring with this inquiry. Key issues confronting current healthcare frameworks, such as information security, security, and constancy, are tended to by this arrangement, which takes advantage of the characteristics of blockchain for secure, decentralized information administration and IoT for nonstop well-being information collection.

Especially, the consider points:

- Actualize IoT-enabled well-being checking gadgets capable of ceaselessly collecting real-time well-being information, guaranteeing exactness, constancy, and secure exchange of data to healthcare suppliers.
- The exactness of the well-being information that has been assembled can be checked by employing a blockchain system. This will guarantee that the data is ensured from unauthorized access and control which as it were authorized people have access to it.
- To empower incite distinguishing proof of variations from the norm in well-being and to empower proactive restorative activities, make a real-time information analytics stage that collects and assesses data from various Web of Things (IoT) gadgets. To assess the coordinates system's usefulness, versatility, and viability in making strides in quiet results and healthcare conveyance, completely test it in genuine healthcare situations.
- Make beyond any doubt that the framework fulfills the most elevated prerequisites for information security and persistent security by assessing its compliance with relevant healthcare rules and benchmarks.
- Assemble input from patients, healthcare experts, and other partners to survey the convenience, acknowledgment, and common satisfaction with the framework, as well as to recognize potential appropriation deterrents and ranges for change.

The objective of the venture is to convert healthcare conveyance and understanding observing, displaying the potential of blockchain and IoT innovation to make a more secure, more proficient, and patient-centered healthcare system.

6.3 Specific Objectives

i. **Design and Implementation of IoT-enabled Monitoring Devices**:

- Vital signs, physical activity, and other pertinent metrics can be gathered in real time with sensors and remote monitoring devices based on the Internet of Things.
- Make sure these gadgets can accurately capture data, send it to healthcare providers securely, and are easy to use.

ii. **Integration of Blockchain Technology for Data Security and Privacy**:

- Implement a blockchain framework to securely store and manage data collected from IoT devices.
- The blockchain system should have strong encryption, unchangeable data records, and restricted access for people with permission.
- Resolve any potential flaws and safeguard patient information against manipulation and improper use.

***

iii. **Development of a Real-Time Data Analytics and Monitoring Platform**:

- Build a centralized platform that instantly gathers and evaluates data from several IoT devices.
- Give medical professionals easy-to-use alert systems and dashboards to help them make prompt medical decisions.

iv. **Evaluation of System Performance and Reliability**:

***

- To evaluate the integrated system's functionality, dependability, and scalability, thoroughly test it in actual healthcare environments.
- Assess the system's capacity to improve patient outcomes, shorten the time it takes for medical interventions to take effect, and deliver precise and timely health insights.

v. **Assessment of Data Security and Privacy Protections**:

- Examine how well the blockchain system protects the privacy and security of data.
- To find and fix such vulnerabilities, do penetration tests and security audits.
- Examine adherence to pertinent HIPAA (Health Insurance Portability and Accountability Act) requirements and standards.

***

vi. **User Acceptance and Satisfaction**:

***

- To assess the system's acceptability and usability, get input from patients, healthcare professionals, and other stakeholders.
- Determine possible adoption obstacles and areas that require development by drawing on user feedback and experiences.

6.4 Traditional System

The conventional framework is utilized to screen the critical physiological states like Circulatory pressure, pulse rate, Thermal reading, and Pulmonary rate utilizing the detectors which are promptly accessible. In this way, the continuous signal values that are detected by the distinctive detectors are at that point given to a microcontroller joined to it. This framework can as it were screen the patient's physical parameters, which cannot be in a crisis circumstances. This makes the quiet to remain within the healing center, increment treatment fetched, and senior people ought to visit the hospital often for checkups. This causes late treatment in a crisis circumstance (Fig. 6.1).

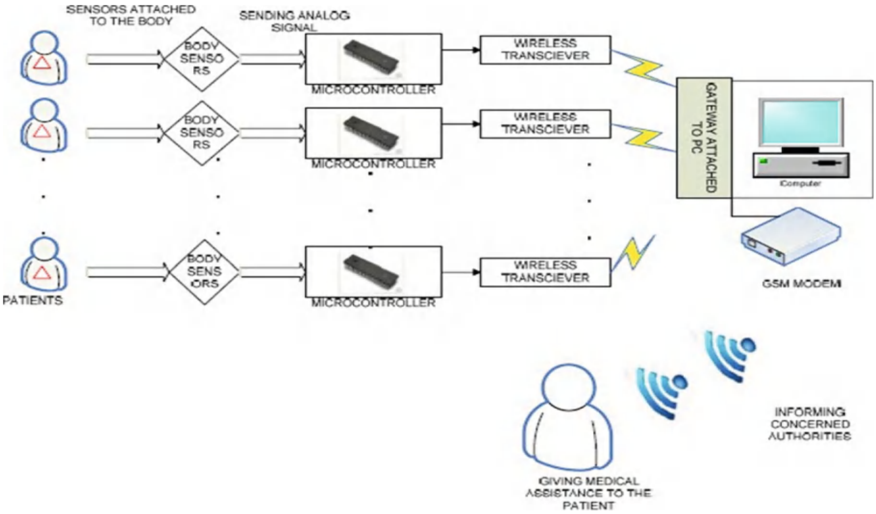


Fig. 6.1 Traditional system

6.5 Workflow Diagram

See Fig. 6.2.

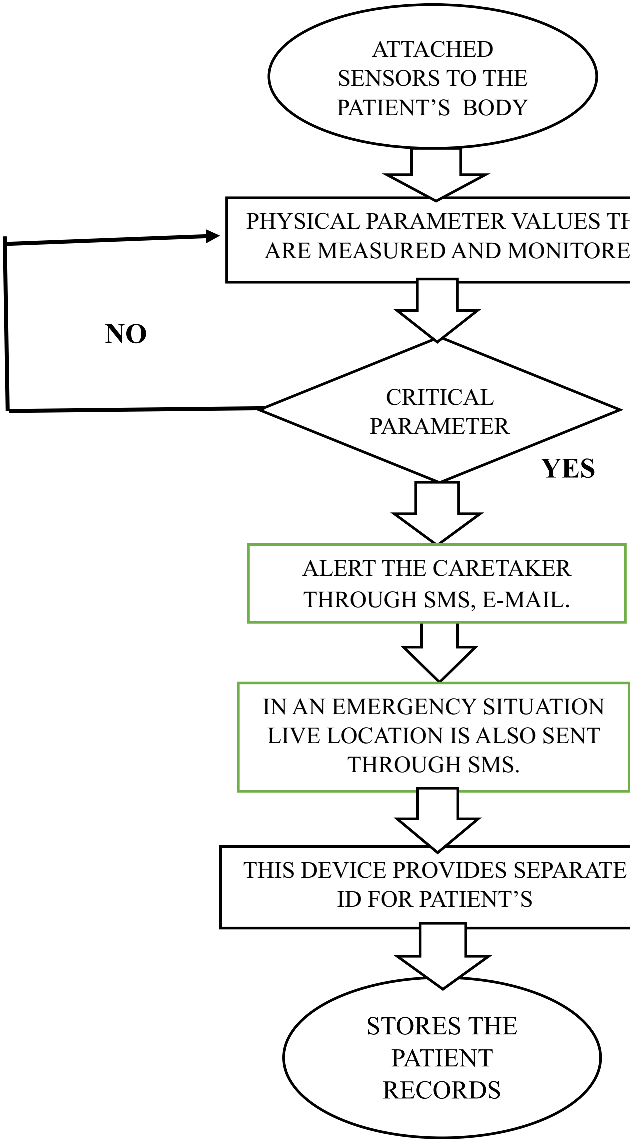

ATTACHED SENSORS TO THE PATIENT’S BODY
PHYSICAL PARAMETER VALUES THAT ARE MEASURED AND MONITORED
NO
CRITICAL PARAMETER
YES
ALERT THE CARETAKER THROUGH SMS, E-MAIL.
IN AN EMERGENCY SITUATION LIVE LOCATION IS ALSO SENT THROUGH SMS.
THIS DEVICE PROVIDES SEPARATE ID FOR PATIENT’S
STORES THE PATIENT RECORDS

Fig. 6.2 Workflow diagram

6.6 Proposed System

The essential objective is to form a quiet observing framework that permits two-way communication, meaning that in expansion to the specialist accepting the patient's information by mail and SMS in a crisis, the doctor may contact the persistent or their gatekeepers by phone or SMS with suggestions that are required. Additionally, Google Maps allows the patient or guardian to follow the patient's whereabouts at all times, allowing for the sending of medical assistance in the event of an emergency for non-bedridden patients. Additionally, a website is developed to analyze the blood pressure, temperature, body movement, glucose level, and heart rate of patients.

6.7 Architecture

See Fig. 6.3.

6.8 Components

(1) Arduino.
(2) Sensors.
(3) Cardiogram.
(4) 2G (Second Generation) mobile network.

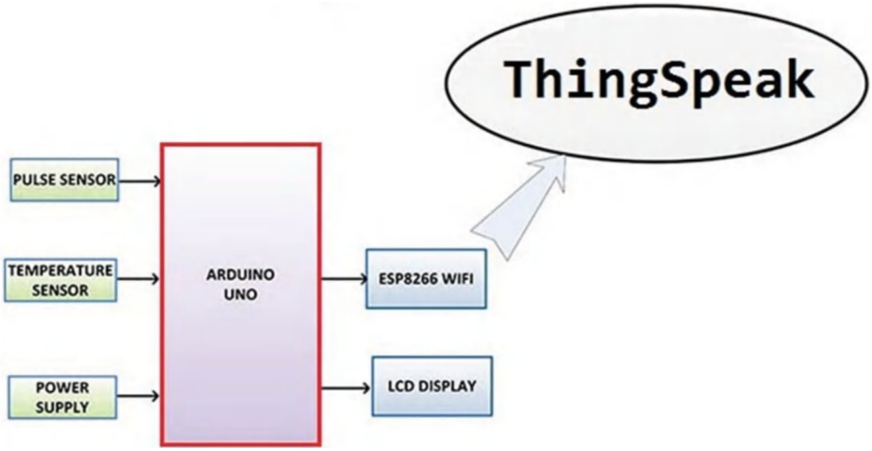


Fig. 6.3 Architecture

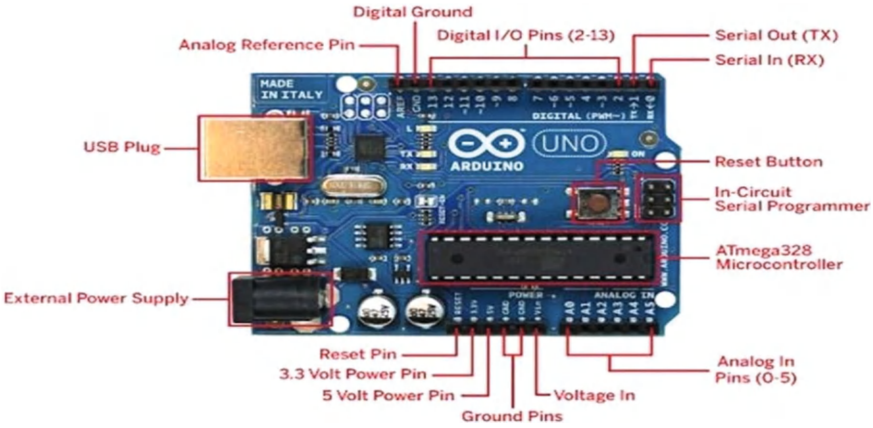


Fig. 6.4 Arduino

(5) Connecting wires.

i. Arduino

One of the most well-known and straightforward sheets that Arduino offers is the Uno. This is due to the ATMega328 microcontroller that it has, which is capable of handling most entry-level applications and is reasonably priced. The open-source electronics platform Arduino is used to develop affordable medical systems and gadgets. It can be applied to many different medical tasks, such as creating assistive technology and keeping an eye on vital signs (Fig. 6.4).

ii. Cardiogram

A cardiogram (ECG or EKG) may be a non-invasive test that screens and records the electrical action of your heart because it beats. Amid the strategy, little plastic patches called terminals are put on particular spots on your chest, arms, and legs. These anodes are at that point associated with an ECG machine using lead wires. The ECG shows the heart's electrical signals within the shape of a chart, which can offer assistance analyze different heart conditions (Fig. 6.5).

iii. 2G (Second Generation) mobile network

Computers and 2G (Second Generation) mobile network frameworks can communicate with one other thanks to 2G (Second Generation) mobile network modules. Most countries use the 2G (Second Generation) mobile network design for flexible communication. The Second Generation (2G) mobile network's expansion, known as Worldwide Bundle Radio Benefit, enables faster data transfer speeds. Second generation (2G) mobile network modules are made up of a 2G mobile network

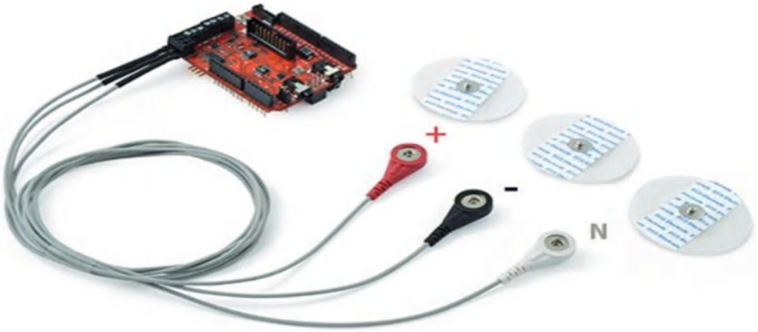


Fig. 6.5 Cardiogram

modem combined with computer connection interfaces (such as USB, RS-232, and others) and control circuits. A class of remote modem devices known as 2G (Second Generation) mobile network modems is designed to enable computer communication with 2G (Second Generation) mobile network systems. Similar to a versatile phone, a Subscriber Identity Module (SIM card) is required for the phone to communicate with the arrangement. Like a flexible phone, it has a unique Universal flexible Hardware Personality number. A 2G (second generation) modem can do the following:

1. Get, send, or erase SMS messages on the SIM card.
2. Perused, included, look SIM phone book sections.
3. Make, get, or dismiss voice calls.

For the modem to communicate with the processor or controller, AT commands must be sent via serial transmission. The controller/processor is the one issuing these directives. The processor, controller, or computer can send various AT commands supported by the modem to establish a connection with 2G (Second Generation) mobile network cellular networks (Fig. 6.6).

iv. **Sensors**

Sensors in healthcare are devices that identify particular natural, chemical, or physical forms and after that transmit or report this information. They can work the exterior of the body or be embedded inside the body. Sensors help restorative experts regulate the right treatment, or can oversee treatment themselves. The essential sensors utilized inside therapeutic gadgets are weight, constrain, wind current, oxygen, beat oximetry, temperature, and standardized tag detection.

(i) **Thermal reading sensor**

A Thermal reading sensor is an apparatus made expressly to gauge an object's heat or coolness. The temperature (in degrees Celsius) is proportional to the output of the precision integrated circuit (IC) temperature sensor LM35. A thermistor is not as accurate as measuring temperature as an LM35. It also has a poor self-healing capacity and raises the temperature in still air by no more than 0.1–55 °C to 150 °C

Fig. 6.6 2G (Second Generation) mobile network

is the operational temperature range. The LM35's capacity to interface with readout or control circuitry is encouraged by its moo yield impedance, straight yield, and culminate inherent calibration (Fig. 6.7).

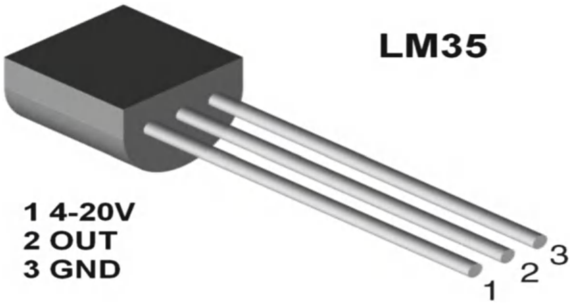
(ii) **Piezometers**

A piezometers is, as its title recommends, a apparatus for measuring and detecting weight, regularly the weight of a gas or fluid. An electronic weight sensor could be a sort of coordinates circuit that capacities as a transducer. It duplicates the flag, which is an electrical flag, in reaction to changes in connected weight. Piezometers, manometers, weight transducers, transmitters, and weight markers are a few other names for weight sensors (Fig. 6.8).

(iii) **Biomechanics Sensor**

Elderly individuals regularly support noteworthy wounds as a result of coincidental falls. This concept employments remote systems and minor, non-invasive sensors to assist elderly and stable people move toward more free living. A network of settled sensors within the domestic environment combined with a little gadget worn around

Fig. 6.7 Thermal reading sensor



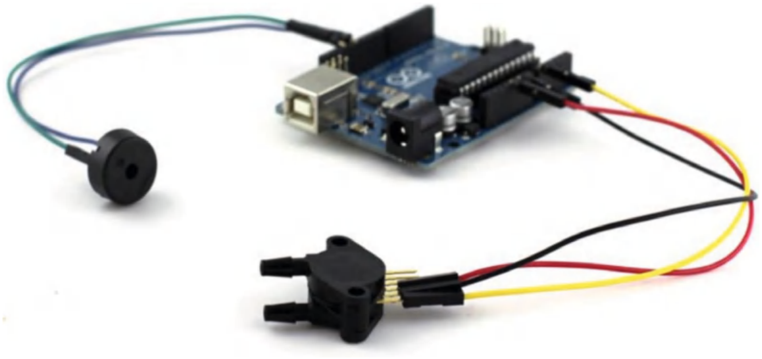


Fig. 6.8 Piezometers

the midriff can distinguish falls and the position of the sufferer. A low-cost, low-power MEMS accelerometer is utilized to distinguish the individual and identify falls based on the quality of the RF flag (Fig. 6.9).

(iv) **Hygrometer**

Since it recognizes, measures, and reports relative mugginess, a stickiness sensor, moreover known as a hygrometer, screens temperature as well as stickiness. The proportion of the real dampness within the discussion to the greatest dampness that it can hold at that temperature is known as relative mugginess. More dampness can be held in higher temperatures. Electrical capacitance serves as the establishment for the

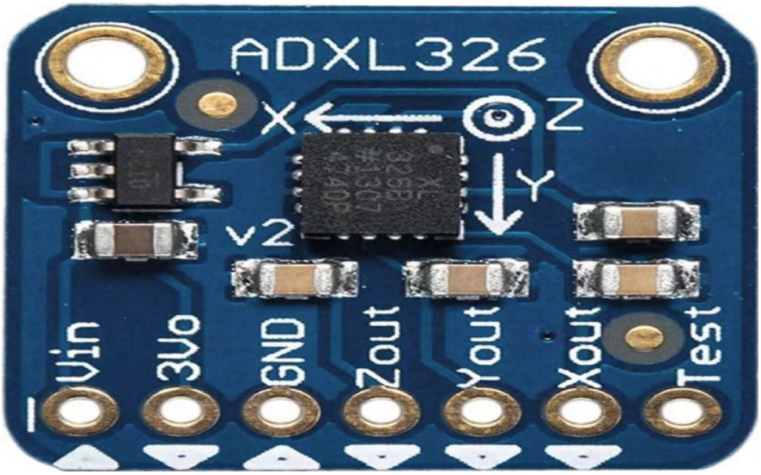
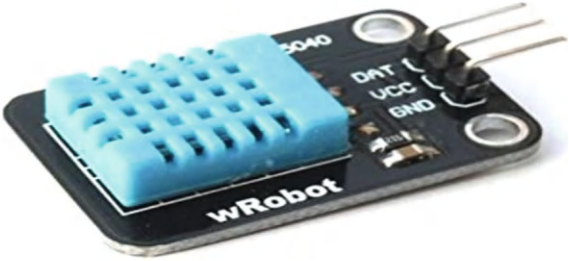


Fig. 6.9 Biomechanics sensor

Fig. 6.10 Hygrometer



capacitive estimation utilized by stickiness and condensation sensors. The capacity of two adjacent conductors to deliver an electric field between them is known as capacitance. The sensor is made up of two metal plates disconnected by a polymer coating that's not conductive. By retaining dampness from the discussion, this layer alters the pressure between the two plates. These voltage varieties are deciphered into an advanced estimation that shows the air's stickiness substance (Fig. 6.10).

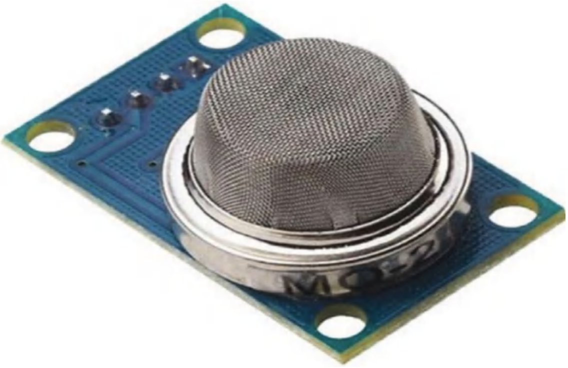
(v) **Toxic gas sensor**

The Gas Sensor (MQ9) module is valuable for finding gas spills in both private and commercial settings. Recognizing LPG, CO, and CH4 makes sense. Its high affectivity and fast reaction time allow estimations to be made as soon as practically possible. The potentiometer can be used to balance the affectability of the sensor (Fig. 6.11).

(vi) **Air quality sensor**

The reason for this sensor is to screen indoors and discuss quality thoroughly. It reacts to several toxic gasses, such as formaldehyde, alcohol, acetone, paint thinner, and carbon monoxide. This sensor's measurement technique prevents it from providing precise information that would allow one to calculate the target gas's concentration. Nevertheless, it has sufficient strength for uses like automatic air circulation systems and refresh sprays that just need qualitative outcomes.

Fig. 6.11 Toxic gas sensor



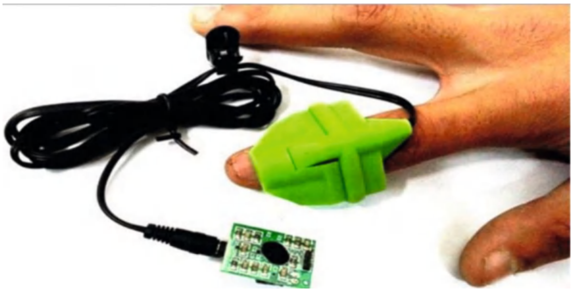


Fig. 6.12 Heartbeat sensor

(vii) **Heartbeat sensor**

The heart rate sensor permits a simple examination of heart work. Based on the principle of psychophysiological signals—which are used as boosters in virtual reality frameworks—the estimate is made. Over time, the amount of blood in the finger varies. A small, very bright light pillar is sent from the ear by the sensor, which then detects the amount of light that reaches a light-dependent resistor. The broadened hail is blended into the circuit and altered. An LM358 OP-AMP is utilized to screen the heart rate from a heart rate sensor, which is utilized to compute the heart rate based on the bloodstream to the fingertip (Fig. 6.12).

6.9 Necessity Examination

Need In order to create any kind of venture successfully, the first and most important step in the program creation process is examination. I started making a list of every feature my application should have. Over the years, there have been a few little adjustments made to the functions. After an assembly with my educator, Daniel Andresen, the taking after necessities has been met for this venture.

a. **System requirements**

- The application must have a module for login utilizing curious capabilities of calm for the master to screen patient's vital data.
- The application must have a module for login utilizing extraordinary capabilities of calm for the Guardian/Caretaker to screen the patient's basic data.

- Region taking after:

The application must have a track region elective with which a master or guardian can track the zone of the calm.

- Range sender:

Gear must have a GPRS module to bring zone organizes which can be utilized to track regions of calm.

- Advising advantage:

Hardware must have a GSM module that sends SMS caution messages to masters and watchmen upon any emergencies. And application must send mail cautions upon any emergencies.

b. **Technical requirements**

The specialized prerequisites of the framework are disconnected from non-functional needs.

- A web application needs to be straightforward, interactive, and easy to use.
- This application should be accessible to inexperienced users with minimal web expertise due to the way the user interface is created.
- It is necessary for users to possess some familiarity with Google Maps.

c. **Computer program details**

- Working System: Windows 7 or higher.
- Organize IoT and blockchain Advancement.
- IDE: Arduino 1.8.4
- Database: MySQL.
- Advancements utilized: C, SQL, PHP.

***

d. **Equipment details**

***

- Board: Arduino Uno
- Sensors: Thermal reading sensor, Biomechanics Sensor, Piezometers, Hygrometer, Toxic Gas Sensor, Air Quality Sensor and Heartbeat Sensor.
- Processor: Pentium IV or higher
- Processor speed: 1.6 GHz
- Smash: 512 MB
- Disk Space: 250 MB or higher.

6.10 Physiological Indicators

Physiological indicators are quantifiable organic capacities that give knowledge into the well-being and well-being of an individual. Cases of physiological markers incorporate:

1. Circulatory pressure.
2. Thermal reading.
3. Oxygen level.
4. Glucose levels.
5. Pulse rate.
6. Thermal reading sensor.
7. Biomechanics Sensor.
8. Piezometers.
9. Hygrometer.

Physiological indicators of wellness display a degree of an organism's reaction to a changing environment.

6.11 Infrastructure Design

The process of describing the layout, constituent parts, sections, interfaces, and data for a framework to satisfy specified requirements is known as a framework plan. The Framework Plan is typically used to illustrate item design, the subsystems that make up the item, and how subsystems are assigned to processors. For displaying framework designs, UML is used. One common object-oriented analysis and plan dialect may be the Unified Modelling Dialect. Use the Case and Grouping graphs, which are UML charts of the application that are displayed below.

I. **Functional design**

A useful plan is made up of a number of parts and their associations. It outlines each conceivable circumstance with respect to how our program interatomic with clients and outside systems to attain its objectives. Entertainers utilize cases, and their connections make up the lion's share of a utilized case graph's components. The utilize case may be a see of the framework from the exterior that highlights a number of activities the client takes to spur the completion of work. The clients who are associated with the application are performing craftsmen (Fig. 6.13).

On-screen characters:

The On-screen characters of the framework are Understanding the caretaker, and the doctor.

Utilize cases:

Based on the features and goals of the application, I have separated out a collection of used situations.

- **Login**: This use case lists the steps that the Subject must do in order to log into the application.
- **Call benefit**: In the event of a therapeutic crisis, this case study demonstrates the steps a doctor must follow in order to contact a caregiver or understanding party.

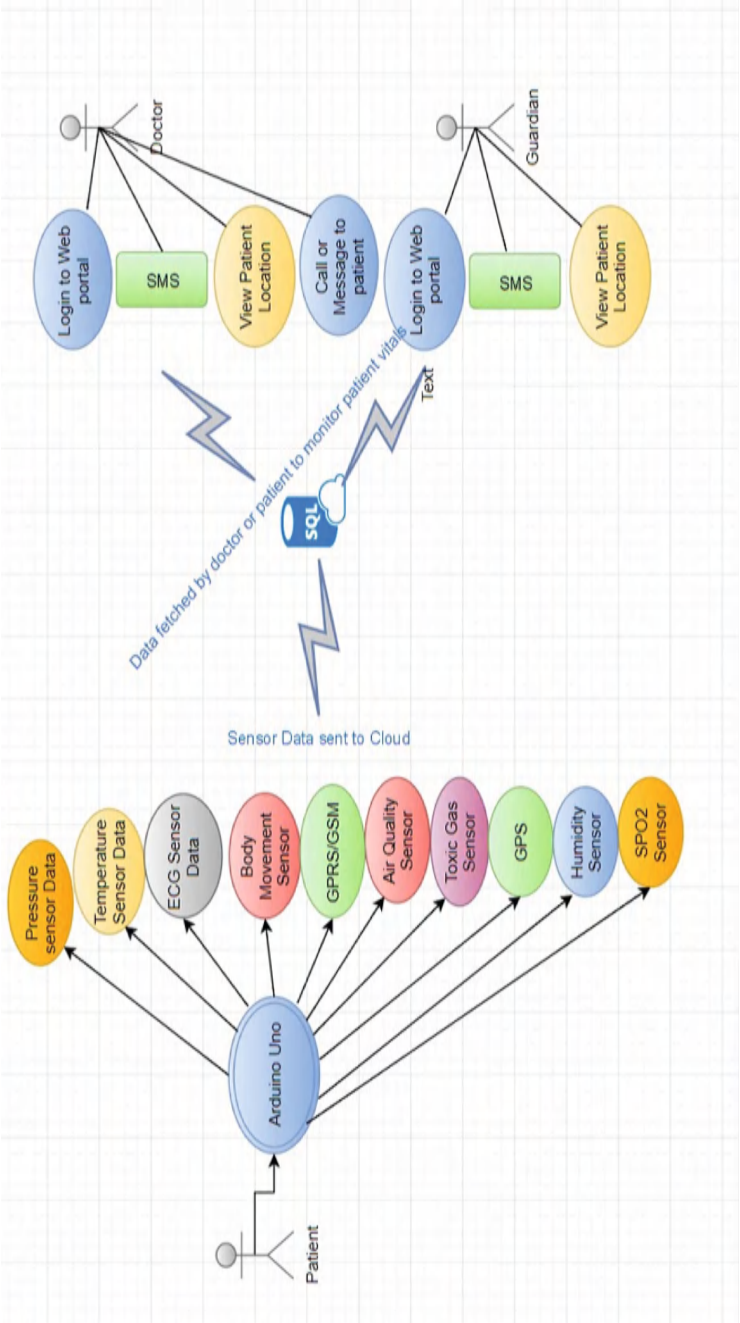


Fig. 6.13 Functional design

- **See region**: This used case denotes a series of actions necessary for the caregiver or physician to locate the patient on a map once they have obtained the delicate aspects of his region.
- **Notifying benefit**: This used example outlines a series of actions that the physician must follow in order to notify the subject's caregiver in an emergency.

II. **Interaction design**

Analysis and design applications of interaction design are common. They enable you to assess and document your reasoning by giving you a visual depiction of the logic flow inside your system (Fig. 6.14).

6.12 Visual Interface

In This project aims to make sure that user interface pages are easy to traverse and that comprehension of them is assumed. Below is a collection of web pages that the user can navigate and explore in further detail.

a. **Access page**

Here is where the patient's unique credentials are entered by the doctor or caretaker. Following verification of qualifications, the login page will be accessed to the Understanding crucial observation page, where the patient's present imperative readings can be seen by the physician or caretaker. To ensure the protection of the persistent information, the professional and caretaker in this case must keep the patient's intriguing qualifications a safe (Fig. 6.15).

b. **Patient's physiological indicators page**

Following a successful login, the physician or caregiver can check the patient's real-time vital signs, such as their temperature, humidity, heart rate, and electrocardiogram (ECG). Patient data is encrypted during transmission to the MySQL database server and decoded during web page delivery to ensure patient privacy. The graphics below provide a detailed explanation of how the patient's current readings are shown on the patient vital monitoring page without any errors. All readings or the corresponding reading in the case of digital values would be displayed as zero if the device was disconnected or if any of the sensors were not linked to the patient. This page would only show the most recent readings that were recorded in the database in the event that the device was turned off (Fig. 6.16).

c. **Live location tracking**

The link to track patient location on the index page can be clicked by a doctor or other caregiver who needs to know the patient's whereabouts. Upon clicking, a Google Maps page including the patient's current location details is displayed. The patient's last known position will be displayed on this page if the 2G module is unable to locate their current coordinates in the device (Fig. 6.17).

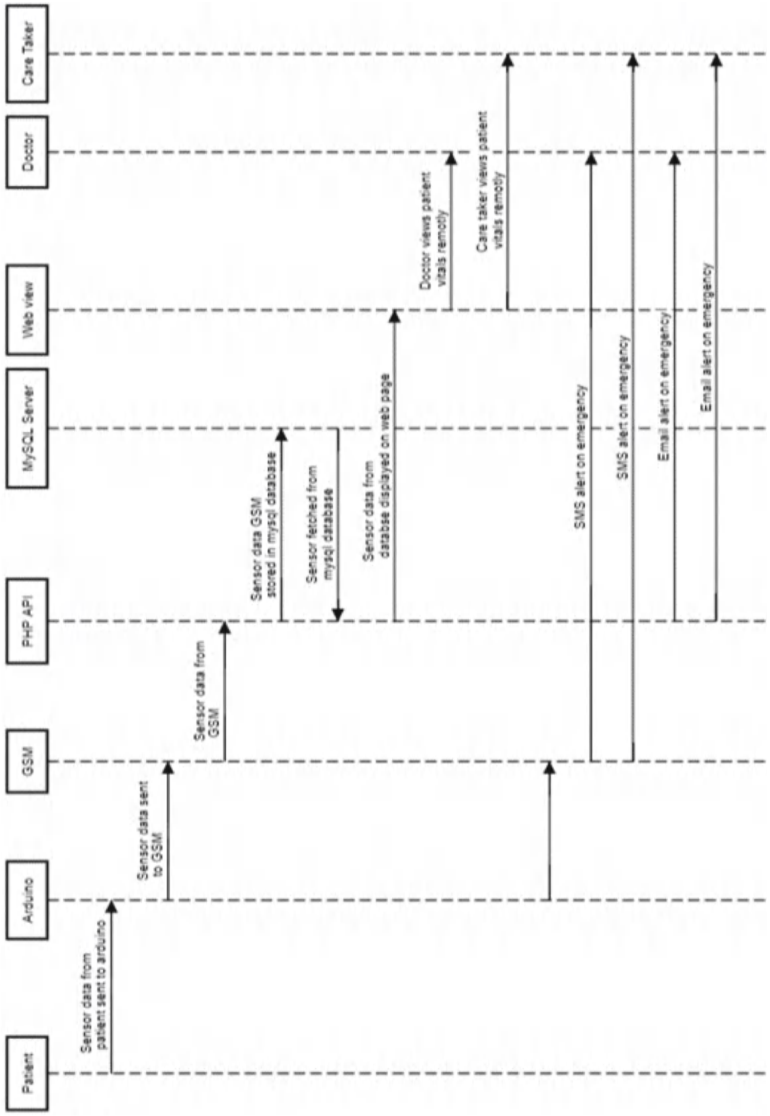

Patient
Arduino
GSM
PHP API
MySQL Server
Web view
Doctor
Care Taker
Sensor data from patient sent to arduino
Sensor data sent to GSM
Sensor data from GSM
Sensor data GSM stored in mysql database
Sensor fetched from mysql database
Sensor data from database displayed on web page
Doctor views patient vitals remotly
Care taker views patient vitals remotly
SMS alert on emergency
SMS alert on emergency
Email alert on emergency
Email alert on emergency

Fig. 6.14 Interaction design

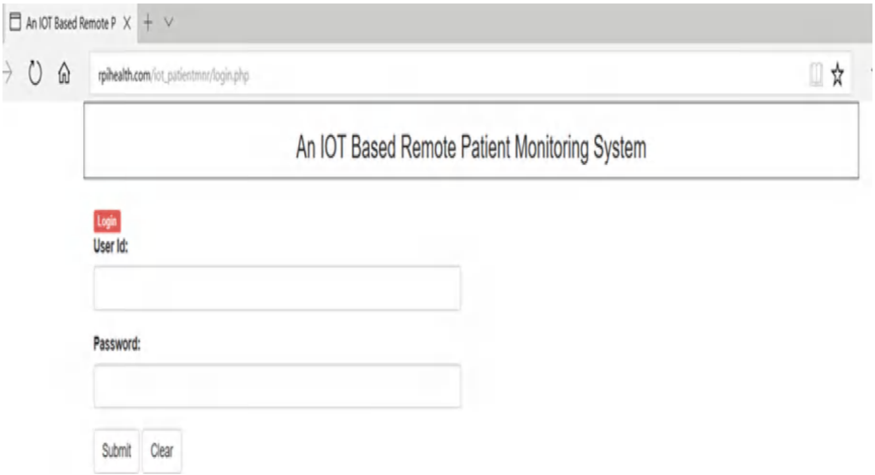

An IOT Based Remote P
rpihealth.com/iot_patientmnr/login.php
An IOT Based Remote Patient Monitoring System
Login
User Id:
Password:
Submit
Clear

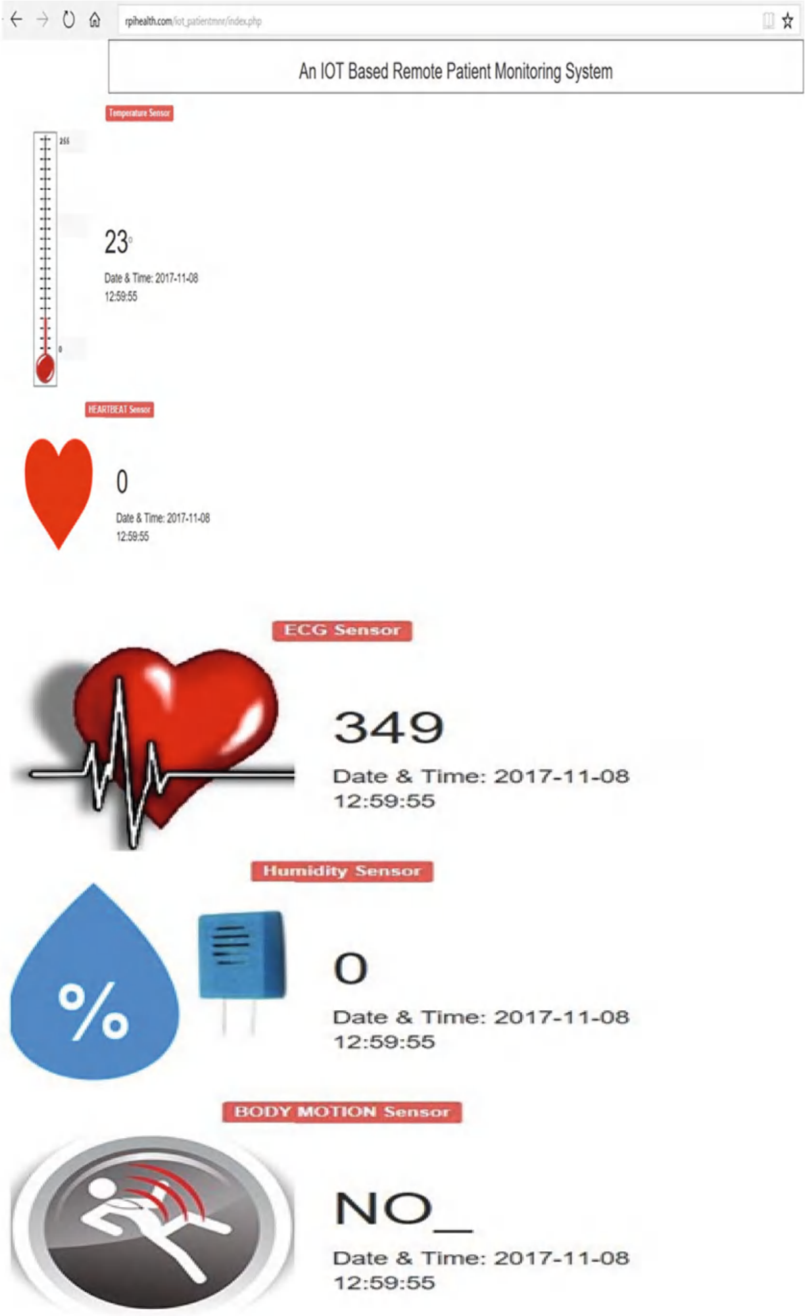
Fig. 6.15 Access page

d. Patient’s Physiological Data

The patient’s physiological history, which has been documented and kept in tabular form on the server, is visible to the doctor here. Doctors can explicitly use this data to analyze patient health conditions and predict any anomalies, suggest changes in medicine or therapies, etc., and even encourage routine patient visits (Fig. 6.18).

6.13 System Configuration

The entire gadget configuration, including the Arduino microcontroller board and power supply connected to it, is seen in the image above. All of the sensors, including the biomechanics sensor for right bottom fall detection, the hygrometer, the ECG sensor, the pressure sensor, piezometers, and the heartbeat sensor, are connected to the microcontroller. The alarm connected to the microcontroller will be activated in the event that any of the sensor data conditions—such as temperature spikes or dangerous gas concentrations—are not met. Additionally, 2G modules are linked, which are utilized to get the patient’s location coordinates and transmit sensor data to a server, respectively. The micro controller is attached to the LCD, which shows a series of information that is displayed as soon as the device is powered up, such as location coordinates and HTTP protocols that demonstrate how to connect to a network. If the device isn’t able to connect to the network, we can diagnose the problem by seeing the command that caused it to halt. After being connected to the network, the gadget displays all patient information and any anomalies in the patient’s vitals (Fig. 6.19).



An IOT Based Remote Patient Monitoring System

Temperature Sensor

23°

Date & Time: 2017-11-08 12:59:55

HEARTBEAT Sensor

0

Date & Time: 2017-11-08 12:59:55

ECG Sensor

349

Date & Time: 2017-11-08 12:59:55

Humidity Sensor

0

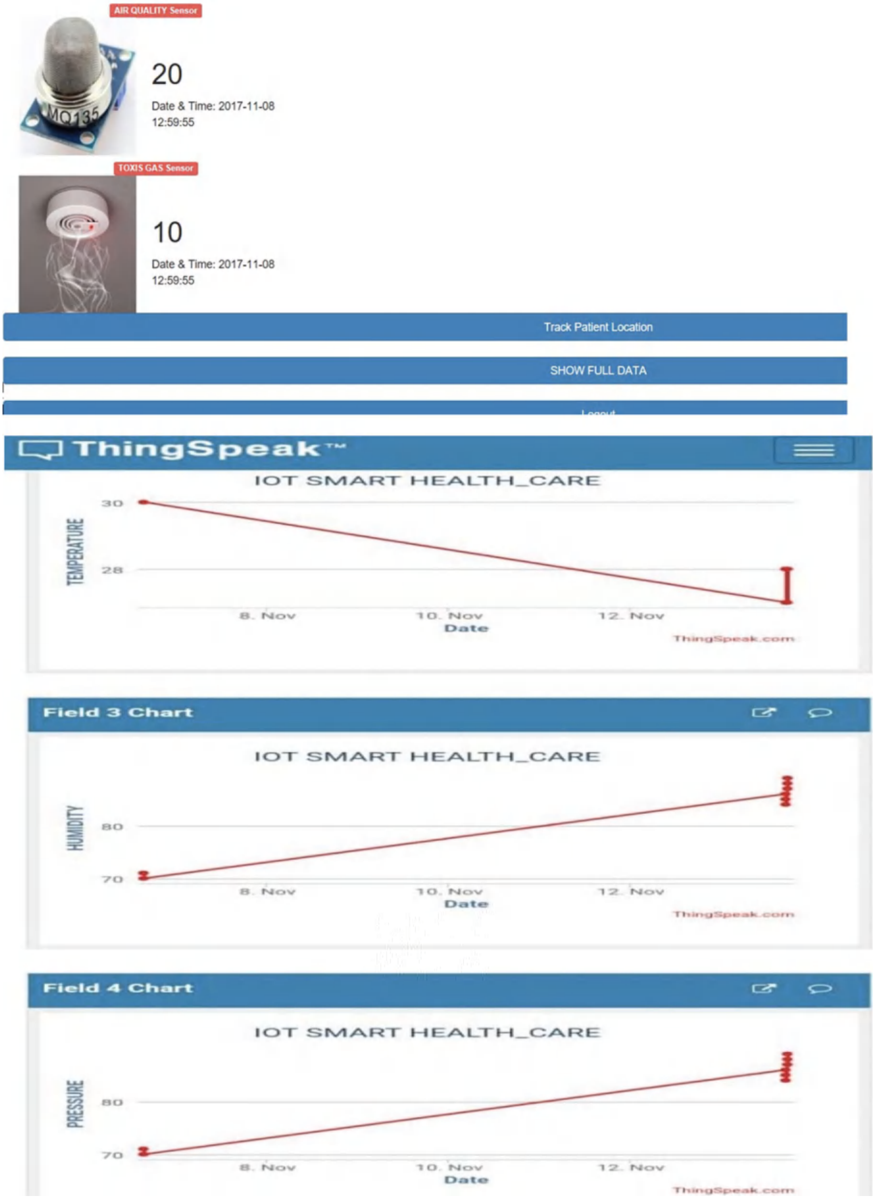
Date & Time: 2017-11-08 12:59:55

BODY MOTION Sensor

NO_

Date & Time: 2017-11-08 12:59:55

Fig. 6.16 Patient's parameter monitoring page



AIR QUALITY Sensor

20

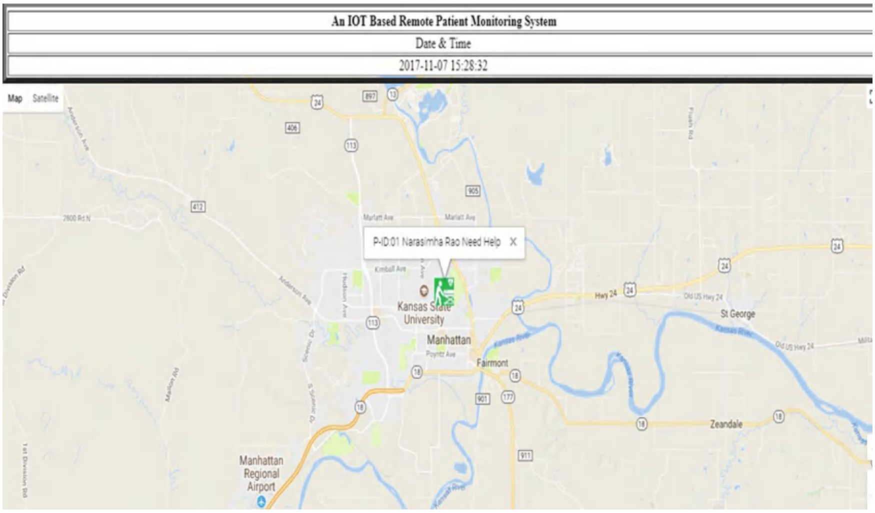
Date & Time: 2017-11-08 12:59:55

TOXIS GAS Sensor

10

Date & Time: 2017-11-08 12:59:55

Fig. 6.16 (continued)



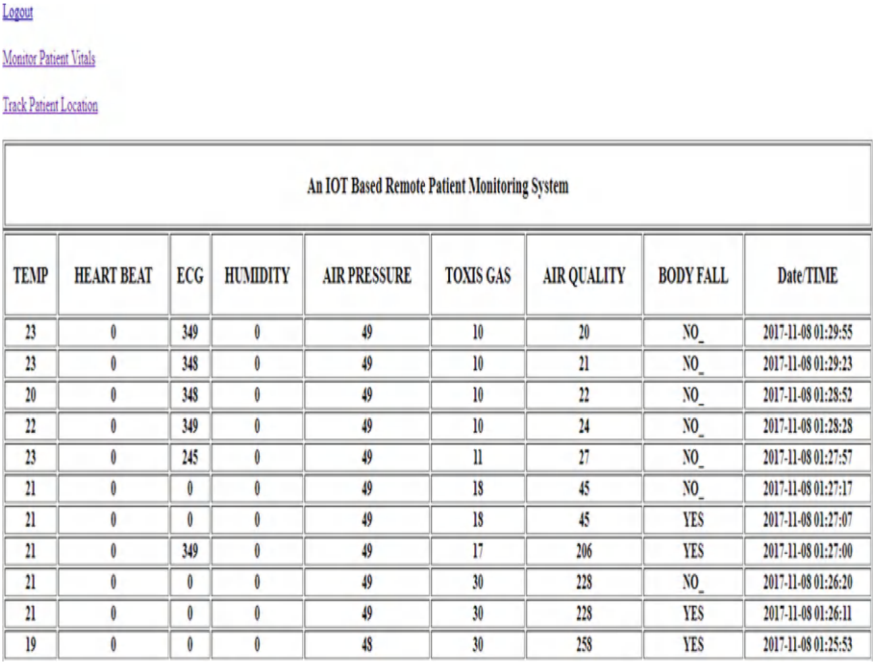
An IOT Based Remote Patient Monitoring System

Date & Time

2017-11-07 15:28:32

P-ID:01 Narasimha Rao Need Help

Fig. 6.17 Live location tracking



Logout

Monitor Patient Vitals

Track Patient Location

An IOT Based Remote Patient Monitoring System

TEMP	HEART BEAT	ECG	HUMIDITY	AIR PRESSURE	TOXIS GAS	AIR QUALITY	BODY FALL	Date/TIME
23	0	349	0	49	10	20	NO_	2017-11-08 01:29:55
23	0	348	0	49	10	21	NO_	2017-11-08 01:29:23
20	0	348	0	49	10	22	NO_	2017-11-08 01:28:52
22	0	349	0	49	10	24	NO_	2017-11-08 01:28:28
23	0	245	0	49	11	27	NO_	2017-11-08 01:27:57
21	0	0	0	49	18	45	NO_	2017-11-08 01:27:17
21	0	0	0	49	18	45	YES	2017-11-08 01:27:07
21	0	349	0	49	17	206	YES	2017-11-08 01:27:00
21	0	0	0	49	30	228	NO_	2017-11-08 01:26:20
21	0	0	0	49	30	228	YES	2017-11-08 01:26:11
19	0	0	0	48	30	258	YES	2017-11-08 01:25:53

Fig. 6.18 Patient physiological indicators

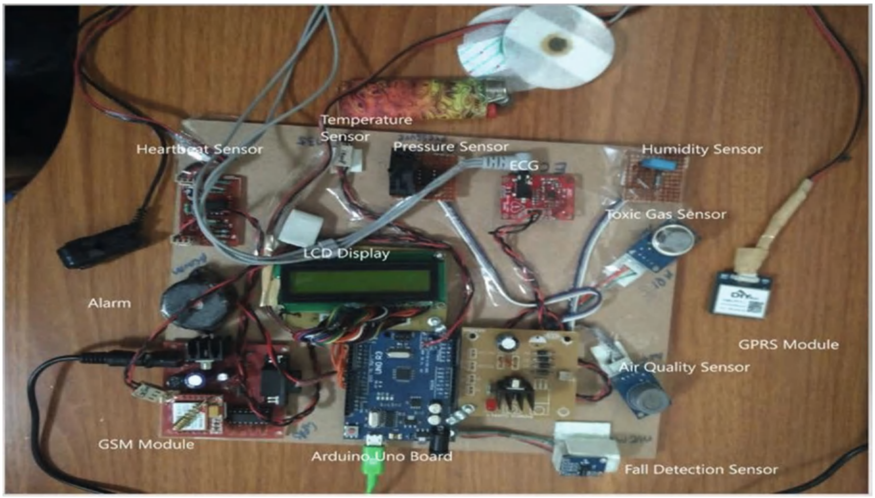


Fig. 6.19 System configuration

6.14 Blockchain Network Setup

Private blockchain network:

- Regulated access and high security are guaranteed by a private blockchain network. Multiple nodes are operated by authorized healthcare institutions and stakeholders.

Consensus mechanism:

- A consensus mechanism, such as Practical Byzantine Fault Tolerance (PBFT) or Proof of Authority (PoA), is implemented to verify transactions and maintain the integrity of the blockchain. Only verified data entries are recorded, this ensures that.

Data encryption and storage

Data encryption:

- All health data collected from Internet of Things devices is encrypted before being transmitted to the blockchain network. This encryption safeguards private medical data throughout transfer and storage.

Immutable Records:

- The blockchain secures every health data exchange, creating a permanent record. The integrity and reliability of patient records are ensured by the fact that once data is recorded, it cannot be altered or deleted.

Smart contracts:

- Data validation, access control, and data sharing are all automated by smart contracts on the blockchain. Data handling complies with security and privacy regulations by executing predefined rules and conditions.

Access control and data sharing

Controlled access:

- Role-based access control (RBAC) is used to restrict data access to authorized personnel only. Healthcare providers, patients, and other stakeholders are granted specific access rights based on their roles and responsibilities. Healthcare providers, patients, and other stakeholders are granted access rights based on their roles and responsibilities.

Data sharing:

- Blockchain technology allows for secure and transparent data sharing among authorized parties. Only verified and authorized requests are granted access to patient data by smart contracts.

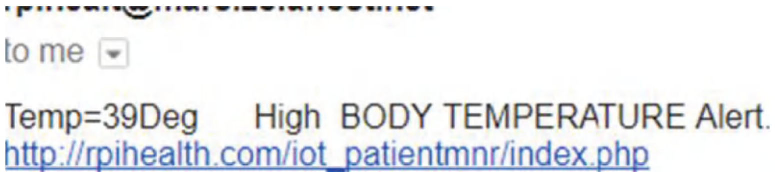
Audit trail:

- A complete audit trail is provided by the blockchain for every request for access or modification. Transparency and accountability of data access and usage are ensured.

6.15 Outcome

Notification via email

An email caution has been sent to the enrolled email with the almost silent vitals and the interface to the quiet observing page.



to me

Temp=39Deg High BODY TEMPERATURE Alert.
http://rpihealth.com/iot_patientmnr/index.php

SMS notification

An SMS caution has been sent to the enrolled email with the data approximately quiet vitals and interface to persistent checking page.

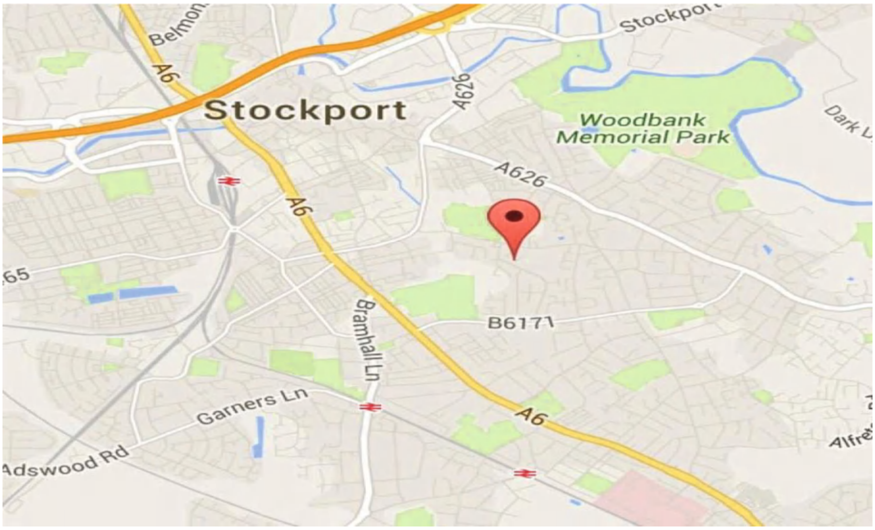
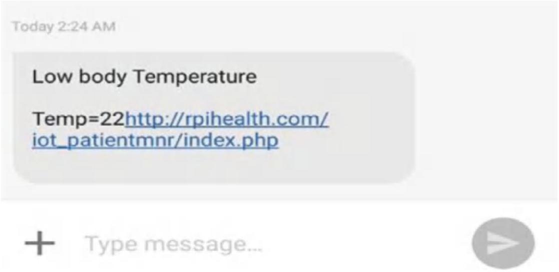


Fig. 6.20 Location tracking


Today 2:24 AM

Low body Temperature

Temp=22http://rpihealth.com/iot_patientmnr/index.php

Location tracking

The patient’s current location is sent to the doctor or caretaker in addition to the text message alert (Fig. 6.20).

6.16 Conclusion

The Secure and Intelligent Patient Monitoring System, which combines blockchain and Internet of Things technology, could revolutionize real-time healthcare delivery by the creation and application of the Secure and Intelligent Patient Monitoring System. There are significant issues with the present healthcare frameworks that this system addresses. Through the use of Internet of Things technology, the system guarantees the uninterrupted and precise gathering of health data from patients, facilitating prompt identification of health irregularities and preemptive medical measures. Blockchain integration ensures the privacy and security of patient data through distributed data administration and encrypted, irrevocable records.

These highlights offer assistance address the pressing issues of unauthorized get to and information breaches that are common in conventional healthcare frameworks. The discoveries appear that innovation improves persistent results by encouraging incite restorative mediations, as well as boosts healthcare conveyance productivity by computerizing information collection and reducing the regulatory stack on restorative experts. The real-time caution framework and user-friendly interface are exceedingly useful and worthy to patients and healthcare experts. The system's versatility and compliance with restorative rules make it a practical arrangement for all sorts of healthcare settings, from minor clinics to sprawling therapeutic educate. The system's capacity to oversee developing information loads without relinquishing execution, at the side the favorable reaction from clients, highlights its potential for wide appropriation and assist advancement. The system's capacity to oversee developing information loads without relinquishing execution, beside the favorable response from clients, highlight its potential for wide appropriation and encourage The Secure and Brilliantly Persistent Observing Framework may be a noteworthy headway in healthcare tech, illustrating how the integration of IoT and blockchain can make a more secure, more profitable, and patient-centered healthcare environment. A modern benchmark for real-time healthcare checking and conveyance is set by this ponder.

Recommendations for future work

(a) The physiological information collection.

    1. Domestic X-rays.
    2. Brain movement checking.

(b) Farther seeing of information is farther.

    1. Issues related with having information online can emerge. Combat disseminated downtime. Information privacy/security particularly of restorative frameworks, and DDOS.

(c) Domestic ultrasound, brain flag observing, tumor location are a few of the inconsistencies that can be identified and collected by the IoT-based inaccessible persistent checking framework.

(d) More research is needed on issues related to online data, data security, and IoT management and operation, which involves multiple technologies and multiple vendors. Security algorithms and certain precautions by the users will help avoid any security related threats in the Internet of Things network.

(e) Which sensors can be used by consumers according to their requirements can be controlled by the interface.

(f) The internet UI can be improved to perform a few exercises, counting controlling the equipment, real-time charts, history, and examination charts to watch irregularities.

References

Query ID="Q4" Text="" Akram SV, Malik PK, Singh R, Anita G, Tanwar S (2020) Adoption of blockchain technology in various realms: opportunities and challenges. Secur Priv 3

Alamsyah MS, Ikhlayel M, Setijadi E (2020) Internet of things–based vital sign monitoring system. Int J Electr Comput Eng (IJECE)

Amir-Ul-Haque Bhuiyan TM, Ahmed S, Salahin Md, Pollab Md, Jui JN, Ahmmed MdT, Anwar Hussen Wadud Md (2023) IoT-based patient monitoring system through online cloud and ECG sensor. IEEE

Atabo GO, Alhassan JK, Abisoye OA, Adeniyi OO, Saidu IR (2023) A review of health monitoring technologies and services. Int J Comput Intell Secur Res

Badamasi S, Oladimeji AT, Ihebuzo NG (2024) Development of an IoT-based device for monitoring vital signs in ambulatory patients. Eur J Biol Med Sci Res

Bae TW, Kwon KK, Kim KH (2020) Vital block and vital sign server for ECG and vital sign monitoring in a portable vital system. MDPI. Sensors

Dwivedi AD, Srivastava G, Dhar S, Singh R (2019) A decentralized privacy-preserving healthcare blockchain for IoT. MDPI

Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener Comput Syst. ScienceDirect 29

Hadiyoso S, Alfaruq A, Tulloh R, Rohmah YS, Susanto E (2021) Internet of things based real-time vital sign monitoring system using mobile application. J Appl Eng Sci 19(3)

Hirekodi AR, Pandurangi BR, Deshpande UU, Ashok Magadum (2020) A survey on IoT based patient vital measuring system. Int Res J Eng Technol (IRJET)

Ibrahim MY, Musa KI, Yarima YA, Ahmad A (2022) A proposed secured health monitoring system for the elderly using blockchain technology in Nigeria. J Electron Comput Network Appl Math

Kuo T-T, Kim H-E, Ohno-Machado L (2017) Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc 24

Li A, Bodanese E, Poslad S, Chen P, Wang J, Fan Y, Hou T (2023) A contactless health monitoring system for vital signs monitoring, human activity recognition and tracking. IEEE

Mahmood AF, Rafaa MM (2022) Designing a collection of two IoT-systems for real time health telemonitoring. J Eng Des Technol

Mohan D, Al-Hamid DZ, Chong PHJ, Gutierrez J, Li H (2024) Fall prediction in elderly through vital signs monitoring – a fuzzy–based approach. IEEE

Patel R, Dwivedi V (2024) A review of secure IoT based smart health monitoring system using blockchain technique. IEEE

Qomariyah NN, Astriani MS, Asri SDA (2021) IoT-based COVID-19 patient vital sign monitoring. IEEE (Institute of Electrical and Electronics Engineers)

Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A (2015) Security, privacy, and trust in the internet of things: the road ahead. Comput Netw. ScienceDirect

Singh R, Gehlot A, Akram SV, Sharma R, Malik PK (2024) Integration of blockchain and the internet of things in healthcare sector. Springer

Uddin MdA, Stranieri A, Gondal I, Balasubramanian V (2021) A survey on the adoption of blockchain in IoT: challenges and solutions. ScienceDirect. Blockchain: research and applications

Yakubu O, Wereko E (2022) Internet of things based vital signs monitoring system: a prototype validity test. Indones J Electr Eng Comput Sci 23:962–972

Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST (2018) FHIRChain: applying blockchain to securely and scalably share clinical data. Comput Struct Biotechnol J. ScienceDirect 16, pp 267–278

Chapter 7
Prospects for Improving the Digital System of the Railways of Uzbekistan Based on Blockchain Technology Based on IoT and Artificial Intelligence

Saymanov Islambek and Rakhimberdiev Kuvonchbek

Abstract In this chapter, the development of railway systems of the Republic of Uzbekistan is studied. Also, models and algorithms for improving the control sensors of the railway crossing signaling system, prospective seamless rail chain control for railway crossing signaling in high and low insulation resistance zones, and means of determining the approach speed of high-speed and high-speed trains to the railway crossing section were studied. However, regulation and management of train traffic, using the Internet of Things at railway infrastructure facilities, IoT reference model according to ITU-T Y.2060, "TETRA" infrastructure, and application of blockchain technology in data storage and information security issues are presented.

Keywords Cryptographic systems · IoT · Railway · Train traffic · Smart locomotive · Blockchain

7.1 Introduction

Nowadays, with the rapid development of information technology and the large-scale implementation of 5G network technology, the Internet of Things has begun to grow at an exponential rate. Electronic health systems, smart cities, smart homes, the IoT for companies, and artificial intelligence that have emerged as a result of this

S. Islambek (✉)
School of Mathematics and Natural Sciences, New Uzbekistan University, Tashkent, Uzbekistan
e-mail: islambeksaymanov@gmail.com

College of Engineering, Central Asian University, Tashkent, Uzbekistan

Applied Mathematics and Intelligent Technologies Faculty, National University of Uzbekistan, Tashkent, Uzbekistan

R. Kuvonchbek
Digital Economy Faculty, Tashkent State University of Economics, Tashkent, Uzbekistan

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2025

K. Ahmad et al. (eds.), *Fostering Machine Learning and IoT for Blockchain Technology*,
Transactions on Computer Systems and Networks,
https://doi.org/10.1007/978-981-96-4074-4_7

development trend are effective and widespread ways to improve various processes for society, such as sensor-based crop irrigation, is gaining importance in harvesting and other automated processes. Such a process strategy reduces the impact of the human factor and helps to increase organizational efficiency, provided that all the conditions for the implementation of IoT technology are met.

Despite its efficacy and popularity, IoT technology faces numerous hurdles and problems related to the security and configuration of IoT devices.

A large number of such devices is problematic because an attacker can get control of them and utilize the Internet of Things devices to orchestrate DDOS assaults and other traffic manipulations that convey device data to the server. A botnet is a coordinated attack on several Internet of Things devices. A botnet is a collection of compromised devices controlled by an attacker (Sadikov 2019; Singh et al. 2012; Tal 1960).

Blockchain and Decentralized approach in the Internet of Things (Internet of Things).

Centralizing the control system of the Internet of Things can be a risk, as it dramatically reduces the time it takes for an attacker to gain control over all devices on the network.

As a solution to this problem, it is necessary to organize the network in a decentralized way, with each technical tool or device acting as an independent node. in this case, malicious subscribers will have to disrupt the operation of all devices on the network, not the main server. But it is technically impossible and an ineffective attack.

Using blockchain technology to provide and manage inter-device communication in a decentralized network is considered to be a very complex process. Because data is delivered in the form of secure, signed transactions that must be stored on each node's distributed ledger. This technique provides the following advantages and features of the interaction of devices in a distributed network (Australian Transport and Safety Bureau 2009).

The benefits of decentralization include safety, identity, network flexibility, autonomy, and information reliability. Decentralization entails addressing the security issues associated with a centralized approach to arranging IoT, which increases inaccuracy while simultaneously boosting network efficiency and security.

Transactions between nodes are considered secure because they are signed with the private key of the transmitting node and verified by the receiving node, which ensures security and identity. Any number of devices can connect to the network at any time and receive an updated copy of the distributed registry, ensuring network flexibility. Autonomy of operation is defined as the inability to suspend the functioning of the entire network by disabling any of its components, as can occur in a centralized network when a server fails. The dependability of network information is based on the fact that the distributed registry blocks will only contain transactions validated by miners or otherwise, as well as the device output information (Sadikov 2019; Mamadiyarov 2022).

Decentralization and peer-to-peer network organization show a high level of security, reliability, flexibility of the network, and the possibility of autonomous operation of its parts.

Proof-of-work is the standard consensus mechanism of the Bitcoin network, which allows you to prove the work you did to confirm transactions and cryptographically complete a block by performing several complex calculations. In a large network, this consensus mechanism is quite expensive in terms of energy spent on block verification and closing calculations. The Internet of Things must support real-time communication and decision-making. This situation proves that the work is useless in solving the problem. Because devices in a closed Internet of Things network must deal with proof-of-work, the network's functionality may be compromised due to the heavy burden placed on devices in calculating proof-of-work.

A miner is a network participant interested in keeping the network running for a reward. A distributed network can be built using proof-of-work; however, only the Internet of Things will be open to external miners. In this case, it is very important to guarantee that miners have enough participation to avoid delays in the creation of new blocks and reduce additional stress on the network nodes. Another option would be to use a lighter consensus algorithm. Following (Mamadiyarov et al. 2022), the preferred and lightweight consensus algorithm for the distributed Internet of Things is Proof of Authentication.

When implementing this algorithm, it is necessary to ensure that the information exchanged between the asymmetric key and the MAC address of the current device is stored in the common communication ledger.

Also, if a trusted node in the network cannot authenticate the blockchain block and the node that sent the block, then the trust score is reduced to 1. If the level of reliability in the network is low, the trusted nodes in the network should be redefined. This algorithm significantly reduces the load on technical equipment. It also makes it possible to ensure the authenticity of the data sent using the electronic digital signature mechanism. Using the above algorithm in addition to the reliable consensus mechanism is effective in ensuring the security of the stored data.

Distributed ledger data can also be implemented using cloud technologies. Therefore, each node also provides access to its own section of the cloud. In this case, the data does not take up space in the device's memory.

In this case, the most necessary data blocks can be stored on the device. Blockchain technology is one of the most effective tools for creating and securing distributed Internet of Things networks. However, the use of this technology has certain limitations:

A distributed ledger can be stored in the cloud, allowing each node to access its own section of the cloud. This ensures that the data does not take up any space on the device.

Also, only the most recent blocks of data can be stored on devices, not the entire data set. This solution allows to abandonment of the interface with the cloud while saving the memory of the nodes.

Using Blockchain technology to build a secure distributed Internet of Things is an exciting and innovative technology.

Standard consensus algorithms are not suitable because they rely on external miners or have high energy costs; however, the Proof of Authentication algorithm provides a reliable consensus process for a network where miners are network nodes. This algorithm can provide the desired device speed and real-time communication. This article suggests two ways to implement data storage.

(1) Give the node access to the cloud-stored copy of the registry.
(2) Store only relevant blocks in node memory to keep the registry light.

High economic efficiency can be achieved by applying these innovative technologies to many economic and social spheres in society. Nowadays, the field of transport and communication is gaining importance in the life of society. In particular, the population of the country uses the services of the railway system of Uzbekistan a lot. In order to improve the provision of better and safer services to the population, it is necessary to organize the activities of this system on the basis of IoT, Blockchain and artificial intelligence, and other modern digital technologies. Therefore, it is important to first analyze this system and solve the issue of safe movement of trains.

At the same time, transport, especially railway transport, is the main component of the industrial and social infrastructure of Uzbekistan. Railway transport organizations transport goods and passengers, store them on the road, load and unload various goods, provide the necessary wagons, clean them and add them to the train, and provide the entire transport process. The general management and operational management of this process is currently carried out by "O'zbekiston temir yo'llari" JSC (Sadikov 2019).

Currently, the transport system of the Republic of Uzbekistan is improving more and more and meets the demand of the population for transport services to the best of its ability. As of 2021, 18,723 organizations are operating in the republic. Compared to 2020, the volume of transport and their services increased to 1947, and the growth was 11.6 percent. In addition, the volume of cargo turnover of railway transport is 18,702.3 mln. t-km., compared to the corresponding period of the previous year, 958.6 mln. t-km or an increase of 5.4% was observed. Geographical location determines the ability of countries to develop. Currently, more than 40 countries of the world do not have access to relatively cheap sea transport services. Including the Republic of Uzbekistan. Therefore, it is necessary to open a wide way to use the services of the Republic and cross-border transit cargo transportation and railway systems. Their trade relations largely depend on the level of development, transit opportunities, and openness of the neighboring countries, and most importantly, their political will. Special attention is paid to this issue in Uzbekistan.

Due to its territorial location, the Republic of Uzbekistan does not have the opportunity to directly use sea transport, therefore it widely uses railway systems in the process of transit cargo transportation with Central Asia and other countries (Sadikov 2019). In recent years, consistent reforms have been carried out in our country to create a modern railway transport infrastructure and to open new trade links to the world market, to create modern railway transport communications connecting our country with other regions of the world. Also, more than 1,200 km of new railway lines were expanded in the republic, and more than 3,800 km of highways were modernized and reconstructed. About 1,100 km of railway networks were fully electrified during the improvement of the introduction of electric trains. As a result, the total length of railways covering all regions of our country was 6500 km.

The UTY network is entirely wide-gauge (1,520 mm). The length of the existing network is 4,718 km, of which 2,530 km (54%) are electrified. UTY uses a semi-automatic block signaling system. The railway lines are in good condition, and the sections between Tashkent, Samarkand, Bukhara, Karshi, and Termez can serve Talgo high-speed passenger trains (Singh et al. 2012). The current railway network is shown in Fig. 7.1.

Cross-border and transit routes. In 2018, domestic transport accounted for almost 33.5% of the turnover and freight volume of Uzbekistan Railways. Also, cross-border transit cargo transportation services make up less than 10% of the total value. In this, the country's import volume increased by 19%, exports by 9%, and freight turnover by 13%. The contribution of transit services to cargo turnover is explained by the distance of railway transit transportation across Uzbekistan (540 km), domestic transportation (227 km), export (258 km), and import (258 km). During Soviet times, it was one of the main railway routes between Central Asia and the Caspian port of Aktau and the part of Russia north of the Caspian Sea. After independence, almost half of the corridor was now a short distance across the border in Turkmenistan, making long-distance transport difficult. Most traffic was redirected to a parallel northwest corridor several hundred kilometers to the northeast in Kazakhstan through Arys and Shalkar (Fig. 7.2).

Based on the above information, it can be understood that now the railway sector of the Republic of Uzbekistan is developing in a fundamentally renewed way. That is, as shown in Figs. 7.1 and 7.2, the volume of railway services is increasing both locally and regionally. The development of methods for evaluating the efficiency of production and economic activity of railway transport is based on scientific and technical achievements, the introduction of new methods of production organization, improvement of economic mechanisms of regulation of internal processes of railway transport in cooperation with external entities.

Railway transport is the basis of the modern economy. In this sense, it serves as an object of market relations, the functioning and development of all branches of the economy, enterprises, their associations and complexes depend on their effective activity. Despite the significant contribution to the country's economy, railway transport is experiencing certain difficulties: to date, the problem of mental and physical wear and tear of the main means has not lost its importance. The decrease in the rate of technical development of the main means of railway transport reduces their reliability and the inconsistency between the parameters of the quality of cargo transport and the competitiveness of road transport in the transport market.

The efficiency, quality and, accordingly, competitiveness of customer transport services are largely determined by the quality of transport processes and the reliability of technical means. Therefore, at present, when establishing modern local and cross-border traffic, first of all, attention should be paid to the issue of safety. In this regard, the effective use of modern OIT, Blockchain and Artificial Intelligence technologies

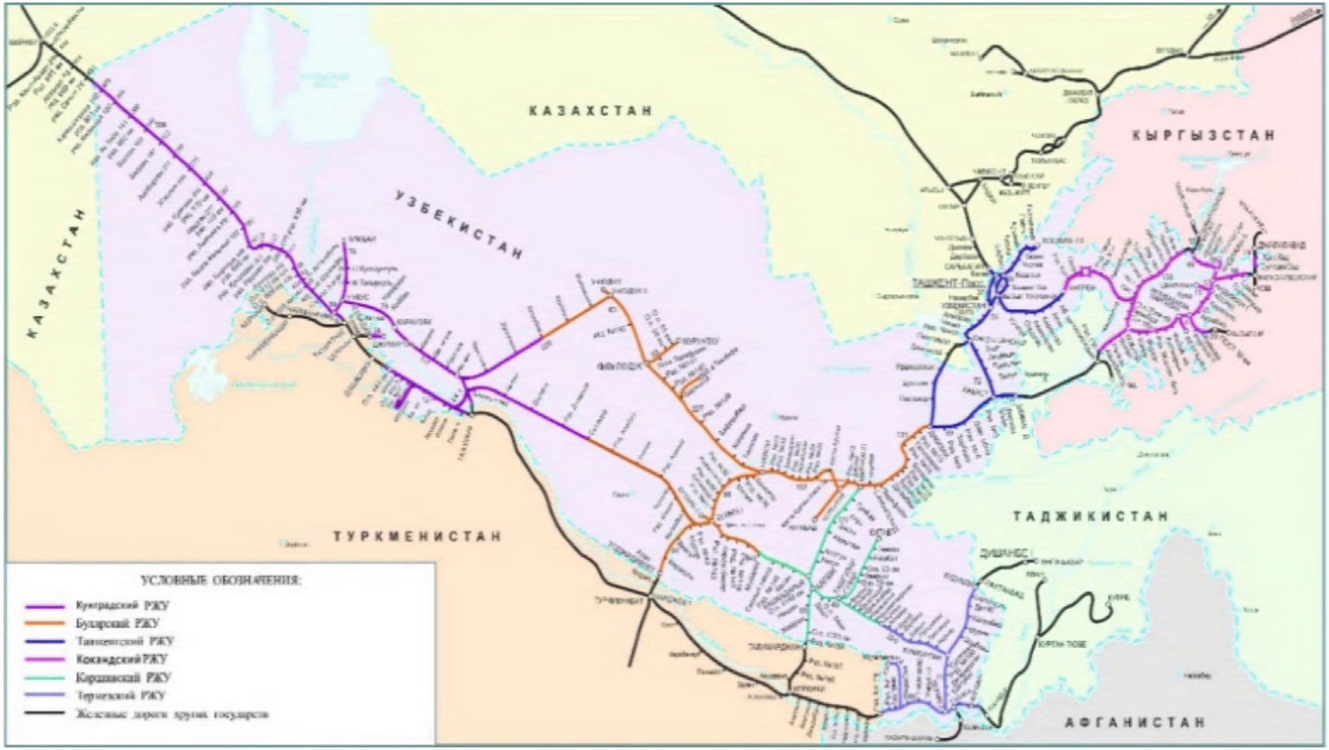


Fig. 7.1 Uzbekistan railway network. *Source* Uzbekistan Railways JSC

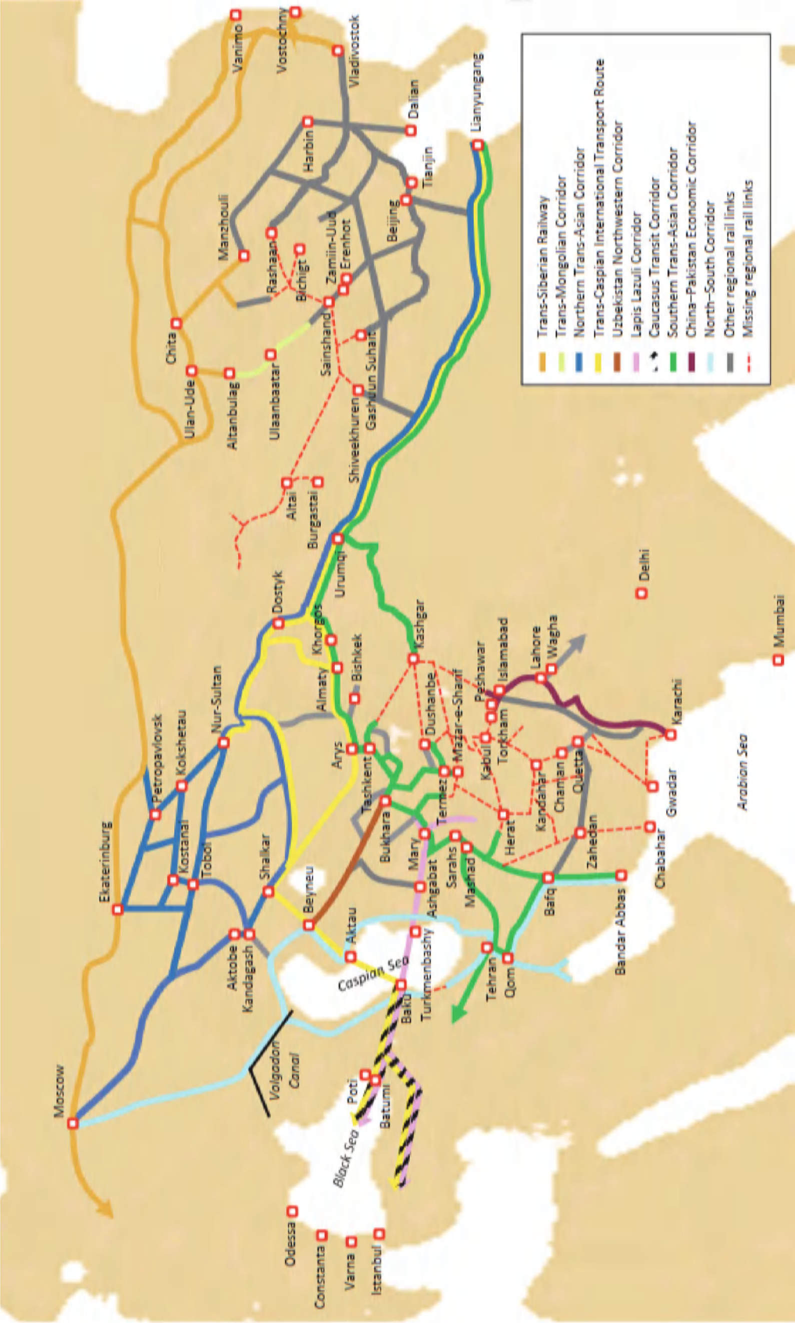


Fig. 7.2 Regional railway lines and ports serving cross-border and transit transport. *Source* TP consultants

to increase the efficiency of train traffic is considered appropriate. Management of train traffic based on these technologies leads to economic and technical efficiency.

7.2 Literature Review

Consistent scientific research is being conducted on the creation of effective local and cross-border systems and the formation of their tasks in various directions. (Sadikov 2019) others made a great contribution to the creation of the national theory of transport process management. In the works (Mamadiyarov 2022; Australian Transport and Safety Bureau 2009; Teramoto et al. 2015), and others, it plays an important role in the formation of the theory of transport and cargo systems, and the design of the placement of transport centers and technical equipment.

Mamadiyarov et al. (2022), Tal (1960), Taggart et al. (1987), Hakkert and Gitelman (1997), Okitsu and Lo (2010) and other famous foreign scientists are dedicated. Also, well-known scientists of our republic M.M. Aliyev, R.M. Scientific works of and Schrader and Hoffpauer (2001) are focused.

The analysis of the results of scientific research showed that safety issues at railway crossings, development, and analysis of statistics of accidents at railway crossings, compliance with technical requirements for the use of railway crossings, signaling at railway crossings basic rules for calculating parameters, calculation of parameters of signaling work at railway crossings, improvement of protective equipment at railway crossings, technical solutions for increasing safety, issues of warning devices and sensor devices at railway crossings. the development and implementation of modern building principles have not been studied enough. The use of IoT technologies in solving these issues leads to effective results (Haque et al. 2015; Hussain et al. 2023; Rempel et al. 2015).

7.3 Analysis and Results

The term “Railway automation and telemechanics” refers to “the field of technology that performs the tasks of regulating the distance and ensuring the safety of trains with automatic and mechanical control methods and tools. At the same time, “the main elements of railway automation and telemechanics technical equipment include signaling, centralization and blocking (BBOB) structures and devices, which include track blocking, electric railway system, centralization of turns and signals, automatic and telemechanics devices of sorting humps, automatic regulation of train movement., dispatching centralization, automatic dispatching control of train traffic, and blocking devices of railway crossings (U.S. Department of Transportation Federal Railroad Administration 2008; Landry et al. 2018; Tilk et al. 2015).

As a system of railway automation (TAT), based on information on the position and speed of various objects, information on track clearance and gauge, management

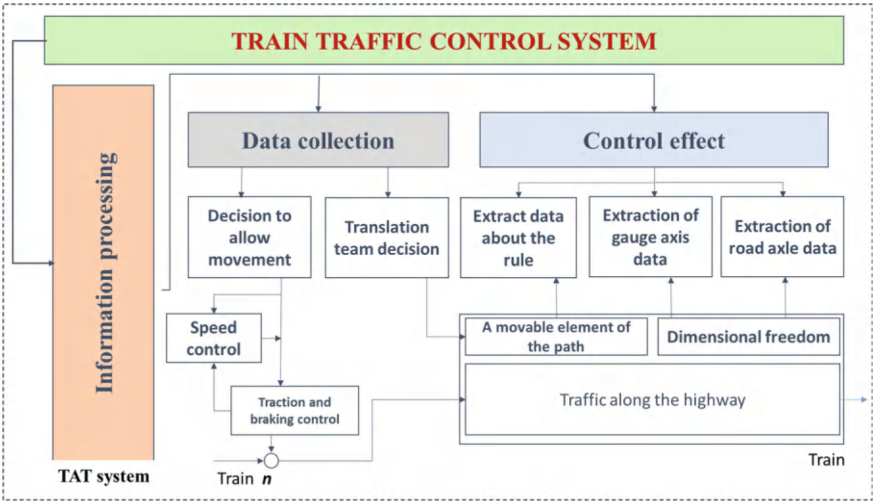

TRAIN TRAFFIC CONTROL SYSTEM
Information processing
Data collection
Control effect
Decision to allow movement
Translation team decision
Extract data about the rule
Extraction of gauge axis data
Extraction of road axle data
Speed control
A movable element of the path
Dimensional freedom
Traction and braking control
Traffic along the highway
Train
TAT system
Train *n*

Fig. 7.3 Control circuit in railway automation and telemechanics system

effects: command to transfer, control of movement, control of traction and braking, etc., the accepted and implemented management circuit is explained (Fig. 7.3) (Haque et al. 2015).

According to Fig. 7.3, the system of railway automation and telemechanics can be represented as a set of lower levels (subsystems):

- track clearance and train location detection systems (axle counters, control mechanisms, etc.);
- systems of distribution of control effects (signaling), including automatic locomotive signaling (ALS) and speed control on railways and rolling stock;
- system of centralization (synchronization of the control system and prevention of wrong control effects);
- information collection, processing and distribution systems (communications system);

This figure also depicts the interrelationship of railway automation and telemechanics (TAT) systems with the train traffic control system (basically, the TAT systems are subsystems for the train traffic control system) and the interrelationship between the goals, tasks and functions of these systems (2005).

In general, railway automation and telemechanics (TAT) systems need to ensure the safe management of traffic processes, that is, the main thing is the security aspect implemented by using protected means and methods of information transmission and processing (Kazakov et al. 1995).

The spatial structure of the railway automation and telemechanics system consists of:

- automation and telemechanics systems at railway stations;

- automation and telemechanics systems in intervals;
- automation and telemechanics of dispatching centralization systems.

At the same time, the structure of railway automation and telemechanics systems can be considered from the position of the functional management structure formed in railway transport (Fig. 7.3). This structure determines organizational and technical elements of railway automation and telemechanics systems and the relationship between them at a significant level.

According to Fig. 7.3, the following levels of railway automation and telemechanics systems can be noted in main road devices:

- twists;
- signals;
- road clearance monitoring devices;
- devices that are activated when a train passes (for example, train devices that indicate the approach to the crossing).

Road devices are connected to control and monitoring sites of nearby centralization posts. At the level of coordination of centralization with track devices, switching of track devices and their monitoring is carried out according to the current train condition (Fig. 7.4).

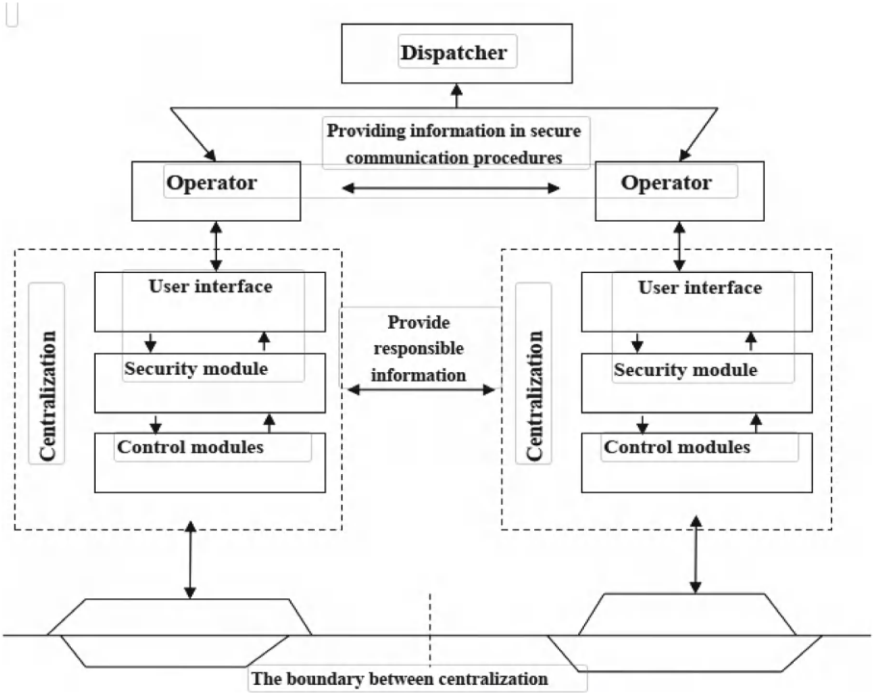


Fig. 7.4 Functional structure of the train traffic control and safety system

At this stage, the role of an operator (on duty, conductor, signalman) works, he is a person directly involved in the preparation of train movement. In addition, it is activated at the pre-planning stage by the requirements of the train traffic management process in railway transport. The operator of this level carries out his duties based on the schedule in which each train movement should be carried out, taking into account the documents (instructions) that correspond to the train schedule, as well as the current train condition. Thus, it will have all the control functions allowed at its level (Mamadiyarov et al. 2024).

It is believed that the ease and efficiency of the operator (on duty) in performing these functions are very different. They depend on the level of development of technical devices used for sending and processing information, as well as partly on the type of system used by centralizing devices. The information needed to inform the operator (guard) about the current train condition depends on the used imaging standards and the system used.

The second level is the level of centralization. For this level, decisions and devices (security module) that prevent errors in the actions/sequences of actions of the Operator by coordinating the decisions made by the Operator are the main ones. At this level, the main function of TAT systems is to prevent unintended operator errors that could endanger the safety of train traffic.

The third level is the dispatch control level. This level is necessary for the synchronization of train movement control by Operators (station attendants). The level of dispatcher control ensures the concentration of all levels of train movement and enables the execution of higher level tasks. In this regard, control technical means in railway transport (dispatcher control centers) support the operation of the dispatch control level. If the centralization posts are connected to the dispatch control centers, there is no need for an Operator at the operational control level, because one person in the dispatch control center performs the work of both the duty officer and the dispatcher. This structure is considered very effective, but it requires a high degree of automation of management processes, compliance of technical devices and reliable methods of information protection. Even though the railway automation and telemechanics systems have the same elements, their structure will be significantly different from each other, which is justified by the significant differences in railway traffic organizations due to macro-environmental factors such as economic, political and climatic-geographical (Saymanov 2024).

Thus, the main and main function (goal) of the railway automation and telemechanics system is to ensure the continuity, continuity and safety of traffic, to protect human life and health, freight and railway infrastructure. At the same time, at the stage of modern development, the required functions of railway automation systems are expanded due to their deep integration with the train traffic control system.

7.3.1 Regulation and Management of Train Traffic

The railway is a large and complex system. It is gradually built, expanded and updated over several years. While new technologies are incorporated into new and upgraded railway lines, older types continue to be used in other areas. Therefore, the service life of railway technologies is usually calculated in decades. The diversity of such technological production of railways increases according to the specific standards of that country. Traditionally, each country developed its national railway systems, which differed to some extent from neighboring railways. For this reason, the technological landscape of Kazakhstan Railways usually consists of many incompatible systems and standards. This applies to electrification, platform track, height and many other things. But this diversity is especially noticeable in automation, telemechanics and communication railway technologies.

This technological diversity is a major obstacle to cross-border train traffic. This problem is particularly evident in sections of the transport corridor where more than 20 train control systems are used (Kabulov et al. 2022, 2024), while the systems often have very similar characteristics and functionality. However, because they are incompatible, the use of cross-border trains is unnecessarily complex and economically unviable. Locomotives must be equipped with several systems of group control and communication, which leads to economic and operational costs. For example, these additional control systems require additional space to be installed on the locomotive, where space is limited. At the same time, they significantly increase the price of the locomotive (control systems can account for 25% of the price of the locomotive), as well as require additional skills for locomotive crews operating different types of systems (2022).

All over the world, the main trend in the development of interval regulation systems is the transition from traditional automation systems based on dividing the interval into blocks (fixed blocks signaling systems) to systems based on the principle of coordinate interval regulation (Kabulov et al. 2022, 2023). In traditional automation systems, a train cannot enter a block until the previous train has left it. According to foreign scientists, such a system lacks flexibility (Kabulov et al. 2023), because the size of the block is the same for all trains regardless of the speed. Thus, the length of the block track necessary for high-speed trains is also used for low-speed trains, which reduces the capacity of the track.

To increase throughput and ensure traffic safety, the English language literature calls it a moving block signaling system (literally, it can be translated as a system with "moving" blocks, and the name Communications Based Train Control is often used). systems based on the principle of adjustment of the so-called coordinate interval have been developed.

An analogue of the European Railway Traffic Management System (ERTMS) is the European train traffic management and signaling standard, the next phase of which consists of the European Train Traffic Management System (ETCS) and GSM-R.

The European Rail Traffic Management System (ERTMS) is the first international standard for ground train control and communication between trains. In the late 1980s, European countries realized that the segmentation of the railway market was becoming a serious problem for the future development of railway transport. The lack of compatibility posed a particular problem for high-speed railways, whose advantages could not be fully realized without cross-border transfers. In this regard, a single standard was introduced for the European railway industry.

ERTMS was originally developed in the EU to connect rail systems across the European continent. The EU has obliged European railways to establish ERTMS through European Council directives and European Commission decisions (Kabulov et al. 2023). However, the advantages of this system made it outstanding for implementation in other countries. Outside Europe, ERTMS is used or planned for use in the following countries: Algeria, Argentina, Australia, Brazil, China, Egypt, India, Indonesia, Kazakhstan, Libya, Malaysia, Mexico, Morocco, New Zealand, Russia, Saudi Arabia, South Korea, Taiwan, Turkey and the United Arab Emirates. Thus, ERTMS is gradually turning from a European standard into a global standard with wide support from all countries of the world (Kabulov et al. 2022).

The main operating principles of the "ERTMS" system are briefly represented by the following elements:

A. On-board controller and driver's terminal. The controller calculates the current value of the braking distance, performs calibration to the inertial coordinate system, calculates the safe distance between trains, the current state of the train in the accepted coordinate system, the current parameters of the movement on the driver's monitor, the state of communication with the dispatcher, the distance to the end of the train moving ahead, displays virtual traffic light indicators, the length of the braking distance. As an on-board controller, it is recommended to use a controller specially developed for the "ERTMS" project.
B. Coordinate system tools. The axle mechanism is used in the odometric odometer system. Installed on each locomotive:

- an axial velocity mechanism for calculating the line speed, instantaneous acceleration and distance traveled of the vehicle;
- doppler radar formation velocity gear. An additional channel of the coordinate navigation system is a Doppler radar that measures speed, acceleration and distance traveled without contact.

The use of data from the two motion parameters mechanism reduces the positioning error of the composition in the inertial coordinate system and increases the reliability of the navigation coordinate system. The integrity of the composition is determined by a device that monitors the pressure in the brake line, determines the coordinates of the last car and sends data to the driver's cab via a radio channel.

The main component of the control center is a system of host computers that is resilient to failures (1oo2D). The safe interval controller consists of a block control core and a safety core, performing all safety functions in the interval. Host computers are connected via a network to jointly monitor hardware and software.

C. Object controller. It functions as a part of the “ERTMS” system at the object control stations and serves to control traffic lights, electric turn signals, and crossing signals, and review the condition of the train. The object controller is designed for the monitoring and control of geographically distributed components and uses in harsh climates and harsh outdoor environments.

7.3.2 Using the Internet of Things at Railway Infrastructure Facilities

The totality of existing automated control systems (ACS), train traffic support systems (TSTS), and Internet of Things (IoT) infrastructure, including digital communication networks and wireless high-speed data transmission, are an integral part in creating a modern platform that will create and improve information management transportation processes on Uzbekistan railways.

Information management integrates both direct management technologies and numerous management and decision-support technologies. The use of the Internet of Things as an information support technology seems to be an integral factor in the development of transport management.

The Internet of Things is a global computer network that combines various types of physical objects that can interact with each other and the outside world. The International Telecommunication Union has developed recommendation Y.2060, which contains a description of the IoT reference model, consisting of four horizontal levels of application, service and application support, network and device levels) and two vertical levels (management and security), covering all horizontal (Fig. 7.5).

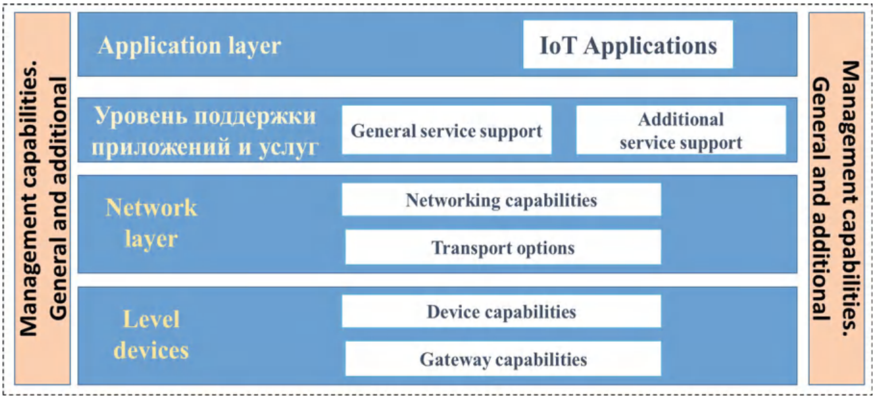


Fig. 7.5 IoT reference model according to ITU-T Y.2060

For the railway industry, the following areas of application of IoT technology can be identified, which can increase labor productivity and the degree of automation of technological processes, reduce production costs, and increase the safety of technological processes:

- monitoring the location and condition of rolling stock;
- control of infrastructure state parameters in real time;
- ensuring personnel safety.

Let us note that ensuring personnel safety by monitoring a person's condition and monitoring his location in dangerous areas in a real-time system seems to be one of the promising areas for using Internet of Things technology.

The use of the Internet of Things when planning a route allows you to take into account information about the weather, and the speed of loading and unloading at specific points along the cargo route, which affects the speed of transportation. Based on real-time data, such a model will be able to build the optimal route and calculate the exact delivery time with much higher accuracy. This means simultaneously reducing costs and delivery times, which will increase customer satisfaction with quality service. Thus, the use of IoT systems increases the coordination of incident management.

The use of sensors makes it possible to monitor the state of distributed railway infrastructure (Mamadiyarov et al. 2022) in real time and predict pre-failure conditions.

The use of solutions in the field of the Internet of Things for railway transport provides an opportunity to implement projects such as, for example, "Digital depot", "Trusted environment", "Smart locomotive", "Condition-based maintenance", "Automated diagnostics of infrastructure and cars." In addition to the use of IoT in the transportation process, it is important to develop control and management of transport infrastructure facilities. For example, a "smart home" system can be taken as a basis using the recently widespread LoraWAN protocol for collecting and transmitting information (Mamadiyarov 2021).

Thus, at such an important railway infrastructure facility as a line equipment room, which houses systems with wavelength-division multiplexing (WDM, wavelength-division multiplexing), it is extremely important to provide the microclimate required for optimal operation of the equipment, which will ensure the installation of the sensor microclimate, fire extinguishing, emergency notification; motion and video surveillance sensors make it possible to control the closed contour of a room; the use of GLONASS sensors allows you to control the movement of infrastructure objects. The list of types of sensors and railway infrastructure objects with which it is possible to equip them in the future can be continued.

In this case, the most important indicator is the energy efficiency of networks, which, according to the recommendation of the International Telecommunication Union (ITU-T L.1310), is defined as "the relationship between a functional unit and the energy required to generate the functional unit," and more specifically, the energy consumption of the sensors themselves (Aripov et al. 2022).

In this area, the published test results from Rohde & Schwarz (Taggart et al. 1987) are interesting, where the battery efficiency of SigFox devices is lower than that of a LoRaWAN device. It is necessary to pay attention to the fact that the energy spent on transmitting a message depends on the time on air and the power of the transmitter. Energy efficiency cannot be compared for systems with different operating ranges. Energy efficiency cannot be compared for systems with different operating ranges. Also of interest is the result of calculating the energy efficiency of a sensor with a Bluetooth (BLE) channel. A BLE beacon with a power of 0 dBm, when transmitting messages with a period of once per second, consumes about 7 μA, and when using a 1000 mAh lithium battery, this sensor will work for more than 16 years, which confirms its energy efficiency (François et al 2011).

Internet of Things systems can use:

- local and personal networks (WLAN—Wireless Local Area Network, and WPAN—Wireless Personal Area Network) with transmission protocols, for example, Wi-Fi and ZigBee;
- global networks (Low-Power Wide-Area Networks) with transmission protocols, for example, LoRaWAN, XNB, 4G LTE, and 5G.

To interact with devices in the railway industry, energy-efficient global LPWAN networks are more often used, providing data transmission over long distances (Table 7.1).

The operating principle of LPWAN is similar to cellular networks. LPWAN uses a star topology, where each device directly transmits data over a radio link to a base station. The station receives signals from all devices within its range and relays the received data to the server using the available communication channel.

The server processes and archives data, and also provides data to users. To ensure global access, users receive data via the Internet or cellular communications. To transmit data over a radio channel, as a rule, an unlicensed range of frequencies is used, permitted for free use in the region where the network is built: 2.4 GHz, 868/915 (LoRa), 433, 169 MHz (Govoni et al. 2015).

The advantages of LPWAN technology are:

Table 7.1 Technology characteristics

Characteristics	Data transmission technologies			
	LPWAN: LoRaWAN, XNB ("STRIJ Telematics")	ZigBee (6LoWPA N)	WLAN: Wi-Fi	WWAN: GSM/U MTS/LTE
Energy efficiency	20 mAh high	Average	Low	Average
Transmission speed data (Data Transfer Rate, DTR), kbit/s	Low 100 bps–1 Mbps	Average 50–200 Mbit/s	High 100 Mbps	High 100 Mbps
Distance, m	10,000	50–100	50	500–1000

- radio signal transmission range (reaches 10–15 km);
- wireless data transmission (does not require laying long cable routes);
- high signal penetration;
- the ability to connect an almost unlimited number of network devices, which allows solving the problem of scaling them and developing the network infrastructure as a whole;
- low power consumption of end devices, due to minimal energy consumption for transmitting a small data packet;
- no need to obtain a frequency permit and pay for the radio frequency spectrum due to the use of unlicensed frequencies (ISM range, Industrial, Scientific, Medical).

LoRaWAN and XNB protocols (Hakkert and Gitelman 1997) are used as transmission protocols in LPWAN networks to solve applied problems, as they are the most common, satisfying the requirements and having the support of terminal device manufacturers. The basis of the transport architecture is the TCP/IP stack.

7.4 Secure Organization of Train Movement Using Blockchain and Cryptographic Methods

The following are important for the safe organization of train movement:

(a) Axle numbering systems. The axle counting system controls the passage of the train through station tracks, it is used to control the unauthorized movement of the vehicle and to determine the emptiness of the road sections, and directional turns. Rail devices register the passage of rolling stock wheels, based on which the axle count monitor determines the number of axles entering and exiting the zone. According to the counters located in the territory, information about whether the territory is free or empty is formed at each counting point.

(b) Peering mechanisms. At the exit from the station, the receiver installed on the rail base transmitters send their docked coordinates on board the locomotive. The use of benchmark mechanisms allows to calibration of the inertial locomotive coordinate system. It is recommended to use passive peering mechanisms that do not require any connection. These mechanisms distribute the information written to them, namely information about their location (Bocchetti et al. 2009).

(c) Information distribution system. These systems can be implemented in a unique way using the IP protocol of this system by the decision of the Scientific and Technical Council of AJ "O'zbekiston Temir Yo'llari". The communication infrastructure is based on the "TETRA" standard trunking communication system according to the decision of the Scientific and Technical Council, which includes:

- management and switching infrastructure;
- subscriber terminals;

The "TETRA" infrastructure includes a device that provides the radio transmission of the "TETRA" network and the necessary modes of operation; switching/routing center; base stations; dispatcher consoles; system control center; other network gateways; application servers, etc. The secure data transfer protocol FSFB2 is used. DMO mode is intended for group interaction between subscribers outside the coverage area of TETRA base stations (Kastell et al. 2006). Communication between subscribers is carried out in half-duplex mode, but the ability to make individual or group calls remains.

The TETRA standard implements the maximum possible frequency efficiency in mobile radio communication systems—4 logical channels occupy 25 kHz. At the same time, the TETRA standard uses Time Division Multiple Access (TDMA) technology along with Frequency Division Duplex (FDD) technology. The type of radio channel modulation is relative differential phase shift keying (π/4 DQPSK) (Kurbonov et al. 2023).

Within the framework of the TETRA standard, network security is provided, aimed at preventing unauthorized use of system resources and ensuring the confidentiality of information sent to the network (Bocchetti et al. 2009).

This is done by the following mechanisms:

- authentication of both subscribers and infrastructure;
- information encryption;
- ensuring confidentiality of subscriber settings;

Authentication of subscribers is carried out based on the main key (K-key) and TEI unique number. A subscriber terminal with an incorrect ID will not be sent to TETRA system resources (Kutsenko and Evdokimova 2022).

Information encryption is an additional feature of each specific system of the TETRA standard. The radio interface of the TETRA standard is considered preprotected. But there may be other encryption applications:

- E2E (End-to-End)—encryption of radio station-radio station private calls (the length of the encryption key can be 128 bits);
- encrypting group calls;
- TEA1, TEA2, TEA3 algorithms (TETRA Encryption Algorithm) radio interface encryption according to.

Confidentiality of subscriber settings is ensured by code protection of the structure of the subscriber terminal and provision of identifier-pseudonyms. At the same time, to create a coordinate interval adjustment system, it is necessary to form requirements for the information transmission system between the locomotive and the control center to perform coordinate adjustment tasks (Mamadiyarov et al. 2023).

(d) Features of interval control systems based on digital radio channels.

PKIR systems with digital radio channels can be conventionally divided into centralized, decentralized and mixed. The centralized type includes, for example, the 2-level ERTMS/ETCS system, which provides for the control of train traffic on an average length of 80 km using a radio-blocking center. In this center, important

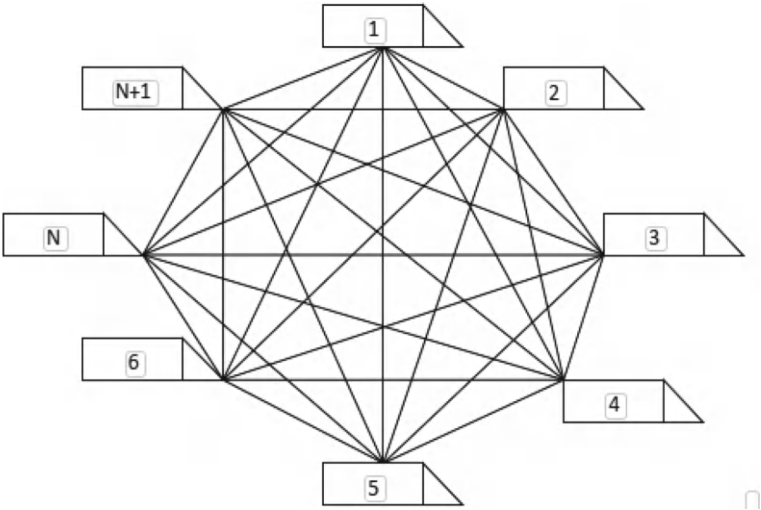


Fig. 7.6 Decentralized (blockchain) traffic management structure

information is processed by a specialized secure computer and then sent via digital radio channels of the GMS-R standard (Ruesche et al. 2008).

At the radio-blocking center, individual traffic speed is calculated for each mobile unit in its area of responsibility, taking into account the general train condition, permanent and temporary speed limits, and track profile.

The proposed system of PKIR, which provides automation of non-stop formation and dispersal operations of unified trains, can be attributed to the decentralized type, its functional scheme is presented in Figure In this system, after receiving the command to perform train connection or disconnection operations through radio channels, all the necessary control and management information is processed in the on-board secure microprocessor control unit (Fig. 7.6).

In mixed systems, the necessary information processing is divided between a specialized secure computer installed in a stationary center and on-board monitoring and control devices. This is, for example, the ITCS system of the General Electric company, where locomotives are equipped with an on-board controller responsible for determining the location of the train with an accuracy of up to one meter, monitoring the integrity of the train, processing information about the state of road devices and monitoring speed limits. A safe logic controller included in the station device of the ITCS system performs the functions of electrical microprocessor centralization (Salmane et al. 2015). The data exchange module with the locomotive device transmits information about the status of signals, turns and crossings to all locomotives in the control area, and the satellite navigation coordinate checking module calculates the geographical coordinates of the trains to the pickets on the track.

In decentralized systems, an important task of the on-board device is the dynamic calculation of braking curves depending on the location of the train, which is performed according to the requirements of documents (Kabulov et al. 2022, 2024). For this, a digital terrain model with the coordinates of anchor points, which can be real or "virtual" balises, as well as generators of rail chains or axis counters, is entered into the on-board electronic map.

(e) Methods of information security in the digital radio channel.

Guided by the technical capabilities of PCR devices, it is necessary to determine the following: the optimal telegram format, and a set of known data protection measures during transmission over an open channel. The means of ensuring security when transmitting information through a radio channel are security procedures and the use of a security code.

Due to the use of the following known protection tools: serial number of the message, timestamp, time control, feedback (receipt), sender and recipient identifier, matching method, security code, and cryptographic methods, the following characteristics related to security are achieved: correctness of the message, integrity of the message, timeliness of the message, sequence of the message. According to the European standard, we make a threat/protection matrix (Table 7.2).

In this, 0 revision, 1 protection.

Since the local radio channel is an open broadcasting system, the following versions of the message are possible.

(1) Data protection is carried out using a distribution code.

Data protection is carried out using a security code, and then encrypted using a key, that is, data is not sent in clear text. Encryption with a key provides protection against intentional falsification and the code—against accidental falsification (Fig. 7.7).

Taking into account the limited resources of on-board devices, we choose "version 1" as the message structure (Fig. 7.7). When using the MOST CM1/MM1 radio station in the 160/460 MHz band, the broadcast code will also perform the functions

Table 7.2 Threat/protection matrix

Type of threat	Protective measures						
	Serial number	Timestamp	Watch the time	Reverse link	A similar clan method	Security code	Cryptographic methods
Repetition	0	0	1	1	0	1	1
Disappearance	0	1	0	0	1	1	1
Connect	0	1	0	0	1	1	1
Change in behavior	0	0	1	1	1	1	1
Distortion	1	1	1	1	1	0	0
Pause	1	1	1	1	1	1	1
Manipulation	1	1	1	0	0	1	0

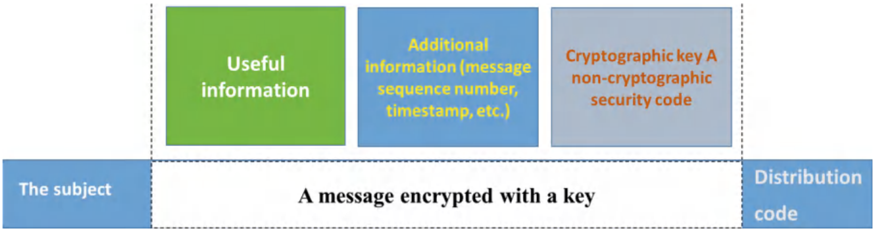

Useful information
Additional information (message sequence number, timestamp, etc.)
Cryptographic key A non-cryptographic security code
The subject
A message encrypted with a key
Distribution code

Fig. 7.7 Encryption with a key protects against intentional falsification

of the security code. When transitioning to the use of network sites (GSM-R/TETRA), it is possible to use the structure of version 2–4 messages.

The most widely used codes for data transmission protection belong to the class of network codes. Network codes provide reliable detection of a certain number of single-bit errors, namely d-1 (d is the Hamming distance). Errors higher than this are determined only with a certain probability. In most cases, the security code is not only required to detect single-bit errors independently. The used non-secure transmission system (GSM, TETRA, DECT) already includes its mechanisms for detecting such errors. The security code should show its activity when the interference effect of the distribution system code is not sufficient or the distribution system is operating through errors. In both cases, it cannot be assumed that only independent single-bit errors occur. In this method of calculating the control expression, polynomial arithmetic is used, that is, binary numbers are represented by formal polynomials with binary coefficients (Zikirbay et al. 2022). This method guarantees the detection of single, binary errors, arbitrary odd-multiple errors, as well as group-type errors, that is, errors that appear in the form of distortion of a certain number of consecutive bits with a group length not exceeding the length of the divider.

Let’s look at an example of data distribution. A stationary device using a local radio channel sends messages to the locomotives located in the area of operation in order of turn and receives message receipts for receiving messages from the locomotives. In addition, in each transmission, the message length M = 252 bits of information contained in the locomotive telegram is coded by the CRC method (resolution is 3, 6, and·10–15), let’s say it is sent to the train at a speed of 900 bits/s (that is, 10,800 messages per hour) via the radio channel. At the same time, the transmission process provides for the retransmission mechanism and the corresponding delayed accounting of the data received on board during the retransmission period.

A dangerous failure during distribution with retry accounting occurs if no distribution error is detected by checking control conditions during the first attempt, or the first error is detected and the second is not detected, or the first two are detected and the third is not found, etc., arises in the case.

According to the CENELEC EN 50,159 standard, the overall efficiency of using a CRC code is estimated with an undetected error probability, where N is the code bit rate. A common value of the failure rate parameter is 10–3, 10–4, and takes into account the average (not necessarily unique) (error probability per transmitted bit.

From here, the error probability in the distribution of length $M + N$ (not necessarily unique) is calculated by the formula $(K + N) \bullet 10^{-4}$.

If so, the probability of a dangerous failure during message transmission is:

$$Q = 2^N Q_1 + 2^{-N} Q_1^2 + \cdots + 2^{-N} Q_1^L = 2^{-N} Q_1 \frac{1 - Q_1^L}{1 - Q_1} \tag{7.1}$$

here, $L = 8$ is the number of allowed repetitions, $Q_1 = (K + N) \cdot 10^{-4}$—message not being sent during the work cycle probability. The intensity of dangerous failure is calculated according to the following formula:

$$\lambda = 10800 \cdot Q = 10800 \cdot 1.57 \cdot 10^{-16} = 1.7 \cdot 10^{-12} 1/\mu \tag{7.2}$$

The advantages of this method include ease of implementation, high productivity, and high probability of error detection. Disadvantages: it is not difficult to write a program that "corrects" the data so that the result is the correct value with a known number of observations. Taking into account the use of open radio channels of information dissemination as an additional channel, it is necessary to use an additional code—a security code formed with the help of hashing algorithms—by the CENELEC European standard terminology. Among such algorithms, the most well-known are the MD5 algorithm (hash length—128 bits), author Ron Rivest, creator of the RSA public key encryption algorithm; and SHA-1 algorithm (hash length—160 bits).

Information security of the TETRA standard system. Information security and information protection issues are some of the most pressing issues in the TETRA standard digital technological radio communication system. These trains are associated with high requirements for critical processes and systems, such as traffic safety management and support systems. The main objectives of ensuring information security in the digital technological radio communication (DRT) system of the TETRA standard are as follows:

- minimization of information risk, economic and other types of losses in case of violation of information security (confidentiality, integrity and availability);
- Coordinate control and interval control of TETRA standard, maintaining the required level of traffic safety when used as an element of train traffic safety levels (ERMTS 2nd and 3rd levels).

Next, we will consider the TETRA (Terrestrial Truncated Radio) radio communication network, which provides voice communication and data transmission and is widely used in special services and large corporations throughout the world. The European Telecommunications Standardization Institute (ETSI) published the first version of the TETRA standard in 1995. The TETRA network works based on the principles of temporary allocation of channels in the 300–500 MHz frequency band, depending on the country, by dividing adjacent channels by a 25 kHz band. The lower transmission frequency range provides a greater radius of operation of base

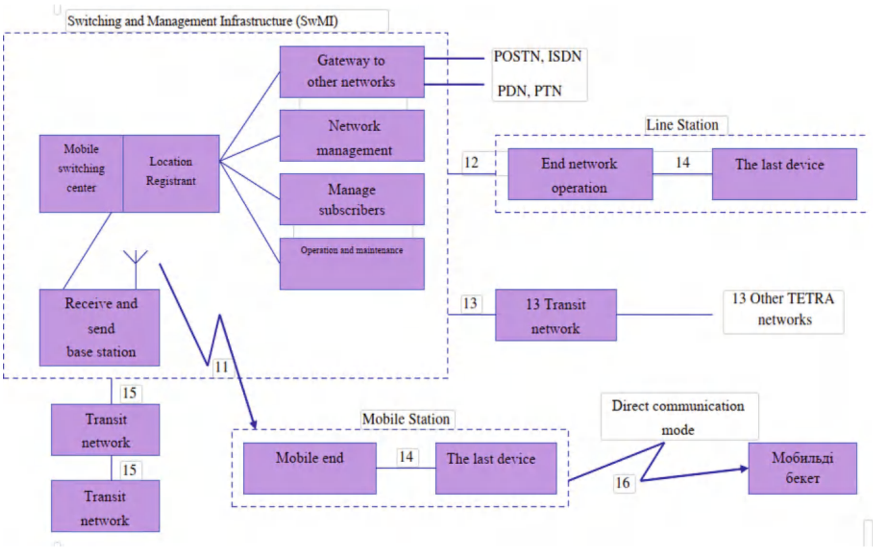


Fig. 7.8 TETRA network architecture

stations compared to GSM. Figure 3.4 shows the network infrastructure of TETRA communication networks (Fig. 7.8).

The TETRA network also provides the transition from one base station to another without breaking the connection. In TETRA, the data transmission speed is 7.2 kbps, and when encryption is used, it is reduced to 4.8 kbps or 2.4 kbps, which severely limits the functionality of the network. The TETRA network can operate in three modes: channel switching, multicasting and SDS short message broadcasting.

The key distribution system of the ERTMS system in the TETRA network is based on modern symmetric cryptographic algorithms, its general scheme is as follows:

The key link in the ERTMS key management system is the key management center (KMB) (Fig. 7.9). KBO is responsible for creating keys for railway transport facilities, including the radio-blocking center and the traction rolling stock that performs the connection to it. The generated keys are used to establish a secure connection between the train and the radio-blocking center. KBO is also responsible for distributing, renewing and deactivating installed keys, because each given key has an expiration date, upon expiration of which one of the mentioned procedures is performed.

When managing the keys of this system, K-KMC keys must first be distributed to all users in the system. The K-KMC key consists of two parts:

- K-KMC1 (192 bits) is used to authenticate KBO and KTCS objects, as well as to confirm the integrity of messages sent by KBO (for example, key management commands). To protect the sent message, the authentication message code (MAS) calculation procedure is used, the result of which is used to check the integrity of the message and the correctness of the message source;

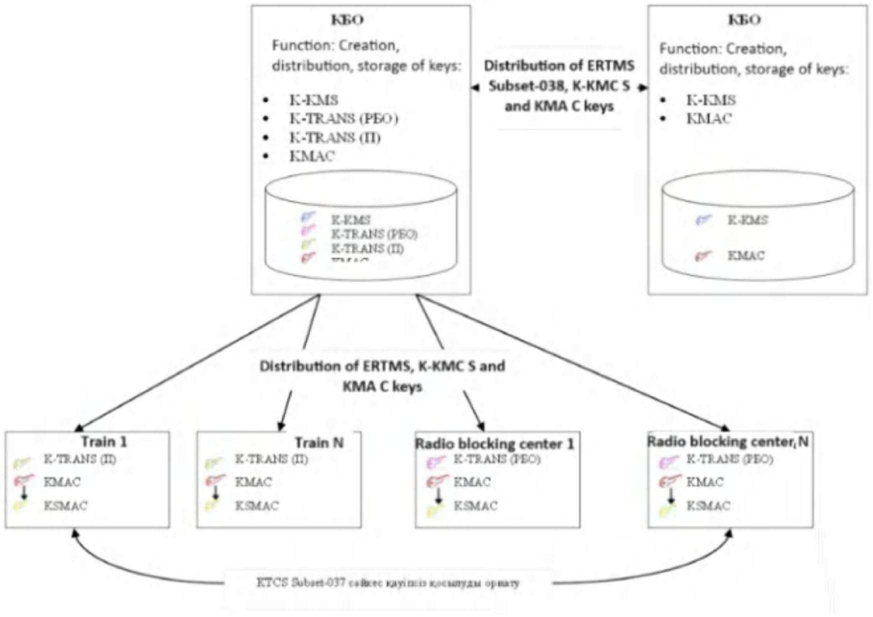

KEO
Function: Creation, distribution, storage of keys:
K-KMS
K-TRANS (PEO)
K-TRANS (II)
KMAC
K-KMS
K-TRANS (PEO)
K-TRANS (II)
KMAC
Distribution of ERTMS Subset-038, K-KMC S and KMA C keys
KEO
Function: Creation, distribution, storage of keys:
K-KMS
KMAC
K-KMS
KMAC
Distribution of ERTMS, K-KMC S and KMA C keys
Train 1
K-TRANS (II)
KMAC
KSMAC
Train N
K-TRANS (II)
KMAC
KSMAC
Radio blocking center 1
K-TRANS (PEO)
KMAC
KSMAC
Radio blocking center, N
K-TRANS (PEO)
KMAC
KSMAC
KTCS Subset-037 сәйкес қауіпсіз қосылуды орнату

Fig. 7.9 ERTMS key management system architecture

- K-KMC2 (192 bits) is used to encrypt second-level keys—authentication keys (KMAC) distributed among all entities of KTCS. Also, K-KMC2 is divided into three subkeys K3, K2, and K1, each of which is 64 bits long. When performing KMAC key encryption/decryption procedures, the key is divided into three blocks, each of which uses the TripleDES encryption algorithm according to the scheme presented in Fig. 7.10.

We can create systems for managing these railway systems and ensuring information security in them. In this case, we can solve the problem of identifying each other by authenticating them when controlling the movement of trains. As a result of this research, mutual authentication models were developed in TETRA radio communication systems.

For the analysis presented in this chapter, we model a TETRA system that includes three main subsystems: user mobile stations (MS), base stations (BS) as the radio access network, and the switching and management infrastructure (SwMI) as the base network that includes the Authentication Center (AuC). The MS forms a physical end device and subscriber identity module (SIM) that is identified with a TETRA device identifier (TEI) and is unique for each device. The SIM card stores the TETRA user/subscriber's unique identification and the associated symmetric cryptographic key in the tamper-proof memory and may implement the cryptographic primitives used in the authentication protocol.

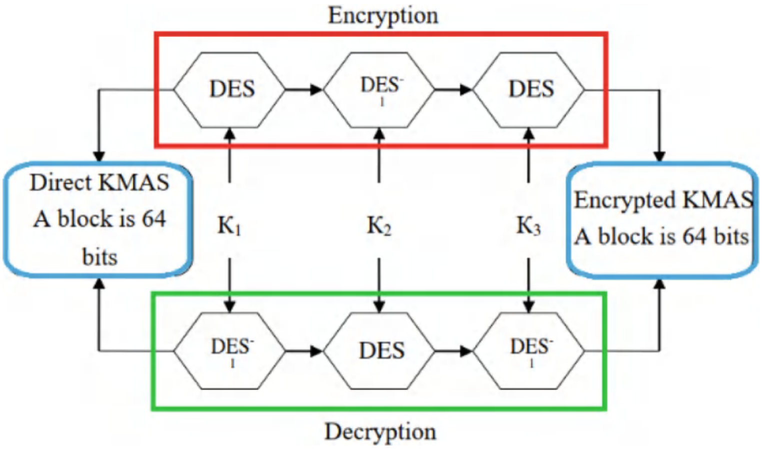

Encryption
DES
DES-1
DES
Direct KMAS A block is 64 bits
K1
K2
K3
Encrypted KMAS A block is 64 bits
DES-1
DES
DES-1
Decryption

Fig. 7.10 Encryption/decryption scheme for authentication keys

The TETRA authentication protocol is specified in (Hakkert and Gitelman 1997). TETRA supports one-way and mutual authentication between terminals and the mobile network, which can be initiated by either. In this work, we will only consider the full mutual authentication protocol, as this is the most significant feature of authentication. In addition, the procedure starting through the network will be considered in detail (Fig. 7.11). However, in weaker one-way authentication protocols, it is possible to simply model the following hits to break authentication as well as MS-initiated mutual authentication (Figs. 7.11 and 7.12).

The parties involved in the authentication process are MS, AuC and BS. It is assumed that the communication channel between AuC and BS is considered secure, and subsequently, AuC and BS can be considered together as one SwMI. One of the main requirements in railway transport is safety.

Ensuring data protection in management systems is considered a task affecting system security. Therefore, the data transmitted through the radio channel should be protected from unauthorized influences and distortions. When considering system security, possible threats are analyzed. According to the EN 50,159 standard, the following risks may occur when distributing information.

- repetition of the message;
- message deletion;
- posting of the message;
- change of message sending order;
- distortion of the message;
- message delay;
- message hiding.

These risks are defined by the European standard EN50159-2 and describe all currently known risks in the transmission of information.

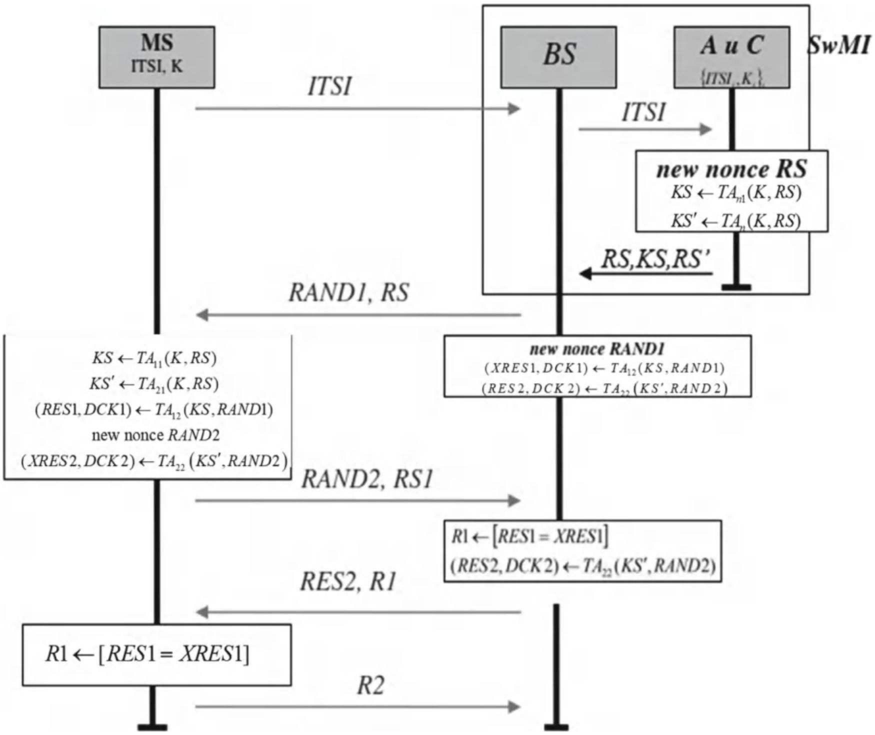

MS
ITSI, K
ITSI
BS
A u C
$\{ITSI_i, K_i\}$
SwMI
ITSI
new nonce RS
$KS \leftarrow TA_{n1}(K, RS)$
$KS' \leftarrow TA_{n}(K, RS)$
RS,KS,RS'
RAND1, RS
$KS \leftarrow TA_{11}(K, RS)$
$KS' \leftarrow TA_{21}(K, RS)$
$(RES1, DCK1) \leftarrow TA_{12}(KS, RAND1)$
new nonce $RAND2$
$(XRES2, DCK2) \leftarrow TA_{22}(KS', RAND2)$
new nonce RAND1
$(XRES1, DCK1) \leftarrow TA_{12}(KS, RAND1)$
$(RES2, DCK2) \leftarrow TA_{22}(KS', RAND2)$
RAND2, RS1
$R1 \leftarrow [RES1 = XRES1]$
$(RES2, DCK2) \leftarrow TA_{22}(KS', RAND2)$
RES2, R1
$R1 \leftarrow [RES1 = XRES1]$
R2

Fig. 7.11 TETRA authentication protocol; Mutual authentication initiated by the SwMI network. MS and BS agree on session key TB4 (DCK1; DCK2)

Authentication in the Euroradio protocol used in the KTCS system is carried out based on cryptographic methods. The full description of the implementation of cryptographic protection methods is given in (Hussain et al. 2023). The integrity of the message is protected by a special MAC (message authentication code) message authentication code, which is a number that prevents an offender from falsifying the message in the Euroradio protocol. The MAS value is calculated based on the secret key and the message text. Any change in the message text requires a change in the MAS value, which is calculated using a private key that is not available to the offender. In theory, the function of computing a message authentication code is to randomly map all possible input values to many n-bit output values. The Euroradio protocol uses a block cipher-based method called CBC-MAC as a MAC function. The main idea of the CBC-MAC algorithm is to encrypt a message m using block encryption in the mode of linking encrypted blocks (CBC—cipher block chaining) and discarding all blocks of the ciphertext except the last one. The MAS value for a message consisting of P1,…, Pk blocks is calculated based on the following formulas:

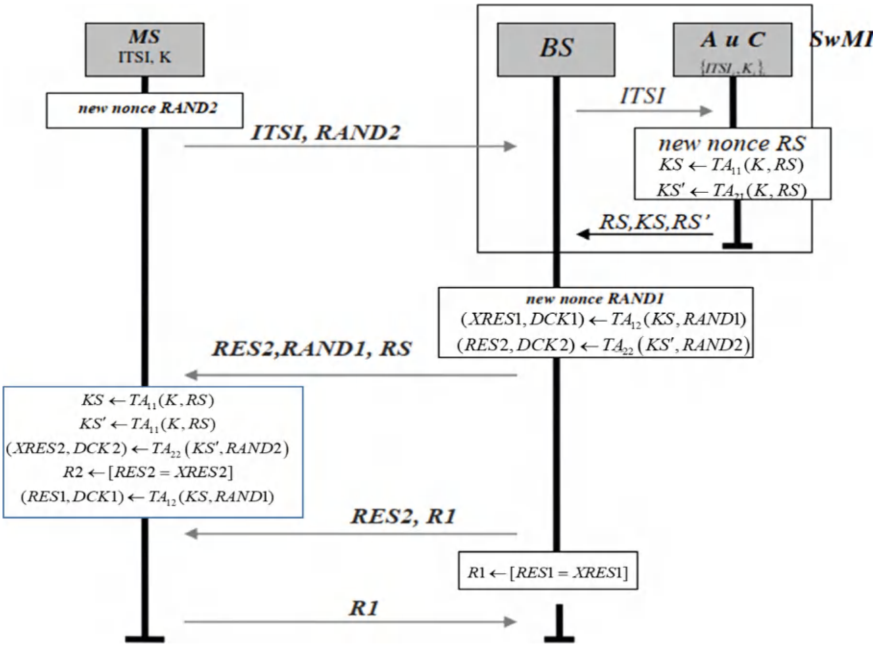

MS
ITSI, K
new nonce RAND2
ITSI, RAND2
BS
A u C
$\{ITSI_i, K_i\}$
SwMI
ITSI
new nonce RS
$KS \leftarrow TA_{11}(K, RS)$
$KS' \leftarrow TA_{21}(K, RS)$
RS,KS,RS'
new nonce RAND1
$(XRES1, DCK1) \leftarrow TA_{12}(KS, RAND1)$
$(RES2, DCK2) \leftarrow TA_{22}(KS', RAND2)$
RES2,RAND1, RS
$KS \leftarrow TA_{11}(K, RS)$
$KS' \leftarrow TA_{11}(K, RS)$
$(XRES2, DCK2) \leftarrow TA_{22}(KS', RAND2)$
$R2 \leftarrow [RES2 = XRES2]$
$(RES1, DCK1) \leftarrow TA_{12}(KS, RAND1)$
RES2, R1
$R1 \leftarrow [RES1 = XRES1]$
R1

Fig. 7.12 TETRA authentication protocol; Mutual authentication initiated by the MS mobile station. MS and BS agree TB4 session key (DCK1; DCK2)

$$\begin{gathered} H_0 = 0 \\ H_i = E_k(P_i \oplus H_{i-1}) \\ MAC = H_{k_k}. \end{gathered} \tag{7.3}$$

During connection, when establishing a session, the authentication procedure shown in Fig. 7.13 is performed.

To determine the MAS, the session key Ks is calculated based on the parameters Ra, Rb and the authentication key Kab according to the following procedure: Ra, Rb numbers are divided into 32-bit blocks.

$$\begin{gathered} R_A = R_A^L | R_A^R \\ R_A = R_B^L | R_B^R \end{gathered} \tag{7.4}$$

The three 64-bit keys Ks1, Ks2, Ks3 are calculated using the following formulas:

$$\begin{aligned} K_{s1} &= MAC\left(R_A^L | R_B^L, K_{AB}\right) = DES\left(K_3, DES^{-1}\left(K_2, DES\left(K_1, R_A^L | R_B^L\right)\right)\right) \\ K_{s2} &= MAC\left(R_A^R | R_B^R, K_{AB}\right) = DES\left(K_3, DES^{-1}\left(K_2, DES\left(K_1, R_A^R | R_B^R\right)\right)\right) \\ K_{s3} &= MAC\left(R_A^L | R_B^L, K_{AB}\right) = DES\left(K_1, DES^{-1}\left(K_2, DES\left(K_3, R_A^L | R_B^L\right)\right)\right) \end{aligned} \tag{7.5}$$

Here $KMAC = (K_1, K_2, K_3)$.

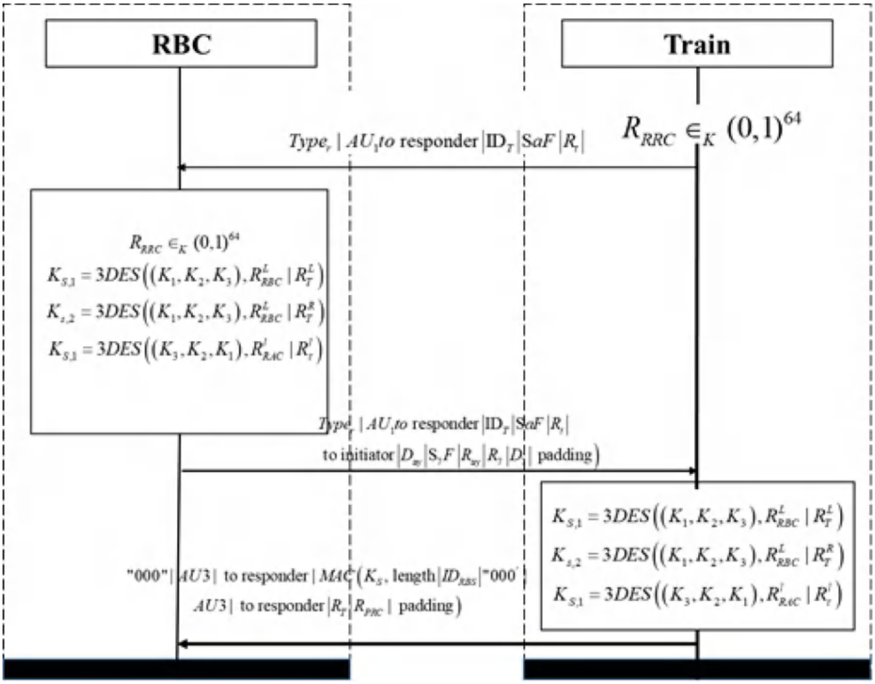

RBC
Train
$R_{RRC} \in_K (0,1)^{64}$
$Type_r \mid AU_1 to$ responder $|ID_T|SaF|R_t|$
$R_{RRC} \in_K (0,1)^{64}$
$K_{S,1} = 3DES((K_1,K_2,K_3),R^L_{RBC} \mid R^L_T)$
$K_{s,2} = 3DES((K_1,K_2,K_3),R^L_{RBC} \mid R^R_T)$
$K_{S,1} = 3DES((K_3,K_2,K_1),R^l_{RAC} \mid R^l_r)$
$Type_r \mid AU_1 to$ responder $|ID_T|SaF|R_t|$
to initiator $|D_{sy}|S_tF|R_{sy}|R_t|D_t|$ padding)
$K_{S,1} = 3DES((K_1,K_2,K_3),R^L_{RBC} \mid R^L_T)$
$K_{s,2} = 3DES((K_1,K_2,K_3),R^L_{RBC} \mid R^R_T)$
$K_{S,1} = 3DES((K_3,K_2,K_1),R^l_{RAC} \mid R^l_r)$
"000"$|AU3|$ to responder $|MAC(K_S,$ length$|ID_{RBS}|$"000'
$AU3|$ to responder $|R_T|R_{PRC}|$ padding)

Fig. 7.13 Key authentication and transformation chain

MAS detection in the radio protocol is based on the use of the TripleDES encryption standard, which is a symmetric block cipher.

7.5 Conclusion

The use of a single cloud platform for data collection and analysis in the Internet of Things technology makes it possible to manage data flows in related technological systems, which is fundamentally different from current operating systems that use a data collection and processing structure isolated within the boundaries of each system. It should be noted that the further introduction of digital technologies, including IoT, in the construction of information management systems in railway transport will improve the quality and volume of transportation.

Also, the following was found during the research. The use of modern systems in the improvement of the railway systems of the Republic of Uzbekistan leads to effective results. Based on the use of known security measures, the following security-related characteristics are achieved: authenticity, integrity, timeliness, and consistency of messages. Information security and information protection issues have been resolved in the TETRA standard digital technological radio communication system. The effectiveness of the proposed algorithms is shown in the architectural model of the TETRA system protocol. An analysis of the multi-level model of secure distribution of information in the European standard system was performed. The exchange of information between the elements of the European standard is given. The GSM-R and TETRA network architectures were analyzed, and the factors influencing the transfer of information from European standard systems to TETRA were determined. A chain of authentication and key generation and MAS cryptographic analysis during data transmission over a radio channel are presented.

References

Aripov NM, Shokhrukh SK, Tokhirov NS (2022) Coals. Practical application of LORAWAN technology for tracking rolling stock in railway transport. Academic Research in Educational Sciences, p 3

Australian Transport and Safety Bureau (ATSB) (2009) Australian rail safety occurrence data. ISBN: 978-1-921602-99-3

Babadzhanov A, Urunbaev E, Saymanov I (2022) Problem of synthesis of minimal forms of logical functions. In: 2022 international conference on information science and communications technologies (ICISCT), Tashkent, Uzbekistan, pp 1–5. https://doi.org/10.1109/ICISCT55600.2022.10146903

Bocchetti G, Flammini F, Pappalardo A (2009) Dependable integrated surveillance systems for the physical security of metro railways. In: Proceedings of the 2009 third ACM/IEEE international conference on distributed smart cameras (ICDSC), Italy. September 2009

François et al (2011) A formal model of requirements. Open Transp J 5:60–70

Govoni M, Guidi F, Vitucci EM, Espoti VD, Tartarini G, Dardari D (2015) Ultra-wide bandwidth systems for the surveillance of railway crossing areas. IEEE Commun Mag. https://doi.org/10.1109/MCOM.2015.7295472

Hakkert AS, Gitelman V (1997) Development of evaluation tools for road-rail crossing consideration for grade separation. Transp Res Rec 1605(1):96–105

Haque K, Fatmi MR, Tanvir S (2015) Effects and feasibility of relocation of kamalapur railway station: an econometric approach. Internet: https://www.researchgate.net/publication/264758593. Accessed 17 May 2015

Hussain A, Khan M, Rakhmonov DA, Mamadiyarov ZT, Kurbonbekova MT, Mahmudova MQK (2023) Nexus of training and development, organizational learning capability, and organizational performance in the service sector. Sustainability 15(4):3246. https://doi.org/10.3390/su15043246

Kabulov A, Baizhumanov A, Saymanov I, Berdimurodov M (2022) Effective methods for solving systems of nonlinear equations of the algebra of logic based on disjunctions of complex conjunctions. In: 2022 international conference of science and information technology in smart administration (ICSINTESA), Denpasar, Bali, Indonesia, pp 95–99. https://doi.org/10.1109/ICSINTESA56431.2022.10041680

Kabulov A, Saymanov I, Yarashov I, Karimov A (2022) Using algorithmic modeling to control user access based on functioning table. In: 2022 IEEE international IOT, electronics and mechatronics conference (IEMTRONICS), pp 1–5. https://doi.org/10.1109/IEMTRONICS55184.2022.9795850

Kabulov A, Baizhumanov A, Saymanov I, Berdimurodov M (2022) Algorithms for minimizing disjunctions of complex conjunctions based on first-order neighborhood information for solving systems of Boolean equations. In: 2022 international conference of science and information technology in smart administration (ICSINTESA), Denpasar, Bali, Indonesia, pp 100–104. https://doi.org/10.1109/ICSINTESA56431.2022.10041529

Kabulov A, Babadzhanov A, Saymanov I (2023) Completeness of the linear closure of the voting model. AIP Conf Proc 2781(1):020020. https://doi.org/10.1063/5.0144832

Kabulov A, Babadzhanov A, Saymanov I (2023) Correct models of families of algorithms for calculating estimates. AIP Conf Proc 2781(1):020010. https://doi.org/10.1063/5.0144830

Kabulov A, Saymanov I, Babadjanov A, Babadzhanov A (2024) Algebraic recognition approach in IoT ecosystem. Mathematics 12(7):1086. https://doi.org/10.3390/math12071086

Kastell K, Bug S, Nazarov A, Jakoby R (2006) Improvments in railway communication via GSM-R. In: Proceedings of the 63rd IEEE vehicular technology conference (VTC 2006-Spring). IEEE, pp 3026–3030

Kazakov AA, Bubnov VD, Kazakov EA (1995) Automated systems for interval control of train traffic. Transport

Kurbonov K, Makhmudov S, Mamadiyarov Z, Khamdamov S-J, Karlibaeva R, Samadov A, Djalilov F (2023) The impact of digital technologies on economic growth in the example of Central Asian and European countries. In: The international conference on future networks and distributed systems (ICFNDS ’23), 21–22 December 2023, Dubai, United Arab Emirates. ACM, New York, NY, USA, 8pp. https://doi.org/10.1145/3644713.3644770

Kutsenko SM, Evdokimova OG (2022) Application of IOT technologies on the path to digitalization of the railway complex. Autom Commun Inform 11:8–10

Landry S, Wang Y, Lautala P, Nelson D, Jeon M (2018) Digital human modeling. In: Applications in health, safety, ergonomics, and risk management, pp 599–609

Mamadiyarov Z (2021) Analysis of factors affecting remote banking services in the process of bank transformation in uzbekistan. Financ Credit Act Probl Theory Pract 1(36):14–26. https://doi.org/10.18371/fcaptp.v1i36.227607

Mamadiyarov ZT (2022) Risk management in the remote provision of banking services in the conditions of digital transformation of banks. In: The 5th international conference on future networks & distributed systems (ICFNDS 2021). Association for Computing Machinery, New York, NY, USA, pp 311–317 https://doi.org/10.1145/3508072.3508119

Mamadiyarov ZT, Sulaymanov SAU, Askarov SAU, Uktamova DBK (2022) Impact of covid-19 pandemic on accelerating the digitization and transformation of banks. In: The 5th international conference on future networks & distributed systems (ICFNDS 2021). Association for Computing Machinery, New York, NY, USA, pp 706–712. https://doi.org/10.1145/3508072.3508211

Mamadiyarov ZT, Sultanova NI, Makhmudov S, Khamdamov S-J, Mirpulatova L, Jumayev A (2023) The impact of digitalization on microfinance services in Uzbekistan. In: The international conference on future networks and distributed systems (ICFNDS ’23), 21–22 December 2023, Dubai, United Arab Emirates. ACM, New York, NY, USA, 11 pp. https://doi.org/10.1145/3644713.3644780

Mamadiyarov Z, Hakimov H, Askarov S (2024) Development of retail banking services in the context of digital transformation. Financ Credit Act Probl Theory Pract 1(54):51–67. https://doi.org/10.55643/fcaptp.1.54.2024.4288

Okitsu W, Lo K (2010) Simulation-free railroad grade crossing Кечикиш calculations. In: Western ITE annual meeting, San Francisco

Rempel et al (2015) System to provide real-time railroad grade crossing information to support traffic management decision-making. U.S. Patent Pending, (Application Number: 15/146,391, Filing Date: May 7, 2015).

Ruesche SF, Steuer J, Jobmann K (2008) The European switch. A packet-switched approach to a train control system. IEEE Veh Technol Mag 3(3):37–46

Sadikov MA (2019) Regulatory and legal aspects of attracting foreign investment to the Republic of Uzbekistan. Young Sci 23:539–541

Salmane H, Khoudour L, Ruichek Y (2015) A video-analysis-based railway-road safety system for detecting hazard situations at level crossings. IEEE Trans Intell Transp Syst. https://doi.org/10.1109/TITS.2014.2331347

Saymanov I (2024) Logical automatic implementation of steganographic coding algorithms. J Math Mech Comput Sci 121(1):122–131. https://doi.org/10.26577/JMMCS2024121112

Schrader MH, Hoffpauer JR (2001) Methodology for evaluating highway–railway grade separations. Transp Res Rec J Transp Res Board 1754:77–80

Sidebottom A (2015) Active control level crossing management, Version 1.01, 01 October 2016

Singh J, Desai A, Acker F, Ding S, Prakasamul S, Rachide A, Bentley K, Nelson-Furnell P (2012) Cooperative intelligent transport systems to improve safety at level crossing. Level crossing, London

Taggart RC, Lauria P, Groat G, Rees C, Brick-Turin A (1987) NCHRP report 288: evaluating grade-separated rail and highway crossing alternatives. Transportation Research Board, NRC, Washington, D.C.

Tal KK (1960) On the methodology for calculating station capacity. Zh.-d. Transp 12:47–51

Teramoto M, Miyaguchi N, Kumasaka K, Ishima R, Fukuta Y (2015) Development of a smart level crossing system for traffic convenience. JR EAST Techn Rev 33:43–48

Tilk IG, Lyanoy II, Redrov YF (2005) Axle counting systems at stations and stretches//Railway transport, p 9

U.S. Department of Transportation Federal Railroad Administration (2008) Driver behavior at highway railroad grade crossings: a literature review from 1990–2006

Zikirbay KE, Alimbaeva ZhN, Alimbaev ChA, Moldash BT, Musilimov DB (2022) System for intelligent metering and management of utility resources based on LoRaWAN technology. Meas Monit Control Control 3:6–19

Chapter 8
Integrating Machine Learning and Blockchain with UAV Routing and Navigation—Challenges and Potential Solutions

Krishnakumar Vaithianathan

Abstract Drones have lots of uses in different areas, but merging them into city airspace brings unique challenges for navigation and traffic control. To tackle these issues, this chapter looks at mixing blockchain and machine learning with drone routing and navigation systems. It dives into two main topics: systems for decentralized drone traffic control and protocols for decentralized coordination, highlighting how blockchain can help drones in communication/routing. Next, it lays out a plan for using blockchain, machine learning, and adaptive routing and navigation together showing how these technologies might team up to make drone operations better. Also, it aims to shed light on the hurdles of blending blockchain with drone navigation networks and the snags that arise when creating and rolling out machine-learning-based drone navigation systems. Some key issues covered include handling data in real-time growth of the system, keeping things private and secure, making different systems work together, following rules, saving energy, and limits on processing real drone data, plus factors like the environment, dynamic cityscapes, and bringing data together. By taking a deep look at these challenges, this chapter gives valuable insights and useful tips for people working on or studying drone navigation to attain sustainable growth in the smart city environment.

Keywords UAV · Routing · Navigation · Blockchain · Machine learning · Smart cities

K. Vaithianathan (✉)
Department of Computer Engineering, Karaikal Polytechnic College, Karaikal, Puducherry, India
e-mail: vkichu77@gmail.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2025

K. Ahmad et al. (eds.), *Fostering Machine Learning and IoT for Blockchain Technology*, Transactions on Computer Systems and Networks,
https://doi.org/10.1007/978-981-96-4074-4_8

8.1 Introduction

Unmanned aerial vehicles, more commonly known as drones or UAVs, have in a very short period of time found their applications from business uses, like aerial photography and package delivery, to the vast universe that includes surveillance and recreational use. Unmanned aerial vehicles are poised to significantly affect the paradigm of infrastructure inspection, emergency response, urban transit, and environmental monitoring, among other smart city applications (Abbas et al. 2023; Mishra and Singh 2023). However, several barriers remain, whether it be airspace congestion, safety considerations, compliance with the law, or privacy. In this respect, innovative solutions that could provide effective and safe traffic control of UAVs in smart city environments need to be considered. After all, with the ever-growing deployment of UAVs, especially in an urban environment, comes a pressing concern for their effective and secure traffic control.

Similarly, in air traffic control, the highly centralized systems that were originally created for manned aircraft are barely coping with the growing number of remotely piloted drones. A stream of drone operations in metropolitan cities, besides being highly concentrated, underscores the current safety, traffic, and regulation infrastructure to be effective. Furthermore, the issues increase in severity due to the highly dynamic and uncertain nature of UAV flight routes that require innovative solutions for traffic management and communication. The use of advanced technology, including blockchains and machine learning, provides promising directions toward the enhancement of routing and navigation systems of UAVs in response to this complex problem. Initially conceived as the financial backbone technology behind cryptocurrencies, such as Bitcoin, blockchain provides a decentralized framework for ensuring the secure recording and verification of transactions between various nodes connected in a network. Its immutability and cryptographic security, combined with its decentralized nature, materialize its suitable use far beyond finance: smart city traffic management for UAVs. It is in this decentralized architecture—operational control and decision-making power distributed among networked nodes—that a sea of change in UAV traffic management (Hamissi and Dhraief 2023; Garau Guzman and Baeza 2023; Alsalami et al. 2024) can happen. Decentralized UAV traffic control systems that are powered by blockchain can promise to take out the drawbacks of conventional, centralized methods. Blockchain-empowered solutions (Barenji and Nejad 2022; Evangeline et al. 2023) can enhance the effectiveness, flexibility, and transparency of regulating urban UAV traffic through a decentralized form of control authority and supporting peer-to-peer communication/coordination between UAVs, air traffic control authorities, and other stakeholders.

What is more, the fact that these types of navigation systems are in place implies that they could be adaptively optimized with the help of machine learning algorithms to take into consideration the variability in the patterns of traffic and circumstances of the environment. Machine learning models can be optimized for route planning, obstacle avoidance, and the process of making decisions through large datasets for better training learned from prior experience. It can overall improve the effectiveness and safety of UAV operations.

The implementation of a UAV navigation network integrated with blockchain and machine learning poses several potential advantages, but many challenges have to be overcome. By several factors, these technologies demand careful thought and strategic planning in the application if they are to have any fruitful use in the real world of the future. These range from technological roadblocks to legal challenges, to personal privacy and security concerns, among many others. Machine learning algorithms (Andreou et al. 2023; Zhao et al. 2023; Chen et al. 2022; Dai et al. 2018) can optimize the operation of UAVs in the smart city context, thereby enhancing safety and increasing the efficiency of traffic management through large data pattern analysis and insight.

This chapter investigates the interaction between three key domains: UAV routing/ navigation, blockchain technology, and machine learning. It stresses the challenges and possible solutions when these key domains are merged. It deals with machine learning-driven adaptive routing and navigation along with decentralized UAV traffic control systems and the problems/challenges related to merging these domains.

The chapter is broken down into four major sections, where each section deals with various aspects of the integration of blockchain and machine learning with UAV routing and navigation systems. The first one details decentralized UAV traffic control systems made possible by blockchain technology and discusses problems arising from the increase in UAV traffic within urban skies. This section also reports how blockchain will facilitate the coordination of UAVs, air traffic control authorities, and other parties in decentralized communication and coordination.

The second part reports machine learning approaches to adaptable UAV routing and navigation. It gives a brief account of the various machine learning approaches available to provide optimized trajectories for UAVs, avoid obstacles, and change navigation strategies dynamically.

The third section details the technological challenges and potential solutions that one may likely have to overcome during the integration of UAV navigation networks using blockchain technology. It probes those areas of scalability, interoperability, security, privacy, and regulatory fit where likely solutions can be contemplated to respond effectively to those challenges.

The fourth and final section is on challenges and likely solutions in implementing UAV navigation systems based on machine learning techniques. Besides the insights into techniques that may counter these difficulties, this includes discussions related to data collection and its quality, robustness of the algorithm, deployment of models, and their validation. The objective of the chapter is to provide a wide view to the reader, of the difficulties and possible solutions while trying to bridge the blockchain technologies and machine learning with UAV routing and navigation systems.

8.2 Blockchain for UAV Routing and Communication

In a few short years, UAVs have rapidly become game-changing technologies that have joined other technologies—infrastructure inspection, crisis management, aerial surveillance, and delivery services, just to name a few—in their maturity. However, this increase in UAVs will equate to more difficult challenges related to traffic management in smart cities; integration into urban airspaces involves complicated and challenging issues. Decentralized UAV traffic control systems (Crann et al. 2024; Hamissi et al. 2023) with the help of blockchain are in a position to come to the rescue of this situation. The increasing number of UAVs flying in crowded metropolitan areas may make it too perplexing for traditional, centralized air traffic control systems, leading to concerns regarding their effectiveness, safety, and regulatory compliance.

In contrast to the traditional model of dependence upon a single centralized authority, a decentralized UAV traffic control system distributes operational control and decision-making power throughout a network of interconnected nodes. The basis of this decentralized architecture is blockchain technology: a distributed ledger system that, when used in a decentralized manner, allows for the safe and transparent recording of transactions and data. Blockchains have been successfully used in many applications: supply chain management (Gurtu and Johny 2019), identity management (Liu et al. 2020), health records (Villarreal et al. 2023), digital asset management (Truong et al. 2023), data management and industry automatization (Vaithinathan and Parthiban 2022), decentralized finance (Schär 2021), legal and governance systems (Vaithinathan and Pernabas 2022), etc.

Blockchain technology thus serves as the basis for decentralized management and coordination of UAV traffic. Every UAV, ATC tower, regulatory agency, or any other relevant party is modeled as a node in the blockchain network. All the messages and transactions taking place among the nodes are stored in the blockchain ledger, guaranteeing the integrity, transparency, and immutability of the data to be shared.

Core Components of Decentralized Drone Traffic Control Systems:

- Blockchain agreement methods: Proof-of-stake and proof-of-work protocols ensure the reliability and uniformity of each record on the blockchain. These approaches prevent data tampering by requiring nodes to reach a consensus on the ledger's current state.
- Intelligent Contracts: Self-executing contracts that use predetermined conditions and rules that are stored in code, smart contracts are also an integral part of the decentralized UAV traffic control system. Smart contracts automate many processes of UAV operations in traffic control systems, hence decentralizing and laying the foundation for many operations like flights, authorizations, and access to airspace. For example, a smart contract might automatically give a UAV permission to enter a certain airspace zone once requirements have been fulfilled, such as the payment of a fee or the correctness of credentials.
- Peer-to-Peer Communication: The decentralized system of traffic control for UAVs includes endowment with peer-to-peer communication protocols, which

makes it possible to share up-to-date information about UAVs and to coordinate them with air traffic control towers and other process stakeholders in real time. It is much faster and more responsive because of direct contact means with very low delays in UAV operations, making it more efficient and safer.

Advantages:

- Greater Robustness: Decentralization makes it more robust; this removes mainly the risks associated with a single point of failure. It, therefore, reduces the chances of disturbances through technical breakdowns or cyber-attacks. Correspondingly, it assures traffic flow maintenance in cases where a particular node or subsystem of the unmanned aerial vehicle breaks down.
- Scalability: Since decentralized designs by definition are scalable, they can accommodate the increase of parties and UAVs with no corresponding major increase in infrastructure or administrative load. Decentralized UAV traffic control systems will then easily meet urban airspace management with no problem even as demand for UAV services in smart cities grows.
- High Security and Privacy: The cryptographic algorithms and decentralized consensus procedures involved in blockchain technology provide a high degree of privacy and security to the UAV traffic data. The UAV operators would be able to have safe private data communication—without any loss of integrity and confidentiality—to authorized parties, which includes flight plans, payload information, etc.

Challenges/Considerations:

- Compliance Regulations: The most critical challenge faced by any decentralized system of UAV traffic control is the need to comply with current aviation norms and standards. To this aim, and considering the special features of blockchain-enabled management of airspace, looking after safety and security aspects, the regulatory bodies have to adapt their regulations.
- Cooperation with Standardized Interfaces and Protocols: Decentralized UAV traffic control systems have to be compatible with existing infrastructure; this includes conventional air traffic control systems, but not least the UAV communication protocols. The entity thus requires stakeholder cooperation to drive forward compatibility and, more broadly, interoperability across a diverse range of ecosystems.
- Performance and Scalability: The rising number of flying UAVs in urban air spaces requires that any decentralized system for UAV traffic control should scale in performance by accommodating more transactions and messages. These networks can also be made more scalable and efficient through optimization techniques such as sharding and off-chain processing.

Blockchain-empowered decentralized UAV traffic control systems hold immense potential for disruption in urban airspace management within smart cities. It has several advantages concerning conventional centralized models of operational control and decision-making authority, such as resilience, scalability, and security by distributing it over a decentralized network (Keith 2023). In this regard, the most important issues that need to be resolved for the safe and effective integration of UAVs in urban airspace, and the realization of the full potential of decentralized UAV traffic control systems, are regulatory and interoperability concerns at the very least. In the case of blockchain-enabled airspace management, these potential game-changing characteristics can be overcome only by the combined efforts of regulated bodies, business leaders, and technology suppliers to defeat these obstacles.

8.2.1 Decentralized Communication and Coordination

The traditional systems of air traffic management are intended to meet the needs of manned aircraft; hence, they are not suited to the complexity arising from the presence of UAVs in large numbers within a city population. Decentralized solutions could enable the coordination and communication of multiple UAVs among one another and with the authorities in a peer-to-peer manner for air traffic control and many other stakeholders through blockchain technology in a decentralized manner. In essence, blockchain technology (Evangeline et al. 2023; Javaid et al. 2023) is a distributed ledger that does not need a central authority; it allows recording in a way that makes it both transparent and safe to share data across the network. In the smart city, for the question of UAV traffic control, blockchain plays the role of a platform with no main control department, providing real-time coordination, cooperation, and communication between all the authorities running air space management.

Blockchain provides a transparent and safe platform for exchanging real-time flying data such as position, altitude, speed, and trajectory in peer-to-peer communication between UAVs. In this scheme, every UAV in the network will have one copy of that blockchain ledger; this ledger is constantly updated with real-time navigation status and the UAV status of the flight (Hafeez et al. 2023). This uses a distributed ledger so that people share the same data and work with the most recent data available, effectively reducing or even excluding the need for central data storage due to the lowered risk of the data being hampered. Moreover, blockchain makes smart contracts, those that are self-fulfilling the terms of the agreement very transparently interfaced in code.

Obtaining flight data is just one of those numerous tasks of UAV traffic control that could be automated with the assistance of smart contracts. Most of the UAV traffic management functions, such as permission to fly, congestion in air space, and verifying if the imposed regulation is enforced, can be automated through the use of smart contracts. One could, for example, work on a smart contract focused on automatic approval and rejection of flight permissions depending on set parameters for proximity to a sensitive area, weather, or air space restrictions.

Another potential benefit of blockchain technology is the improvement in privacy and security (Sachdeva et al. 2023) for communications among UAVs. Blockchain technology makes assurance in the encryption of each exchanged detail concerning the UAV communication shared with stakeholders. Every transmission within the network is therefore safely done by using cryptographic techniques, therefore keeping delicate information safe from illegal access or interception by some malicious actors, such as flight plans, payloads, and mission objectives. Besides, blockchain technology maintains an indelible record of each transaction and communication over its network; it drives accountability in UAV operations through its transparency. This facilitates greater trust among the involved stakeholders and better surveillance and auditing in UAV operations. Law enforcement and regulatory bodies come in handy with blockchain-facilitated technologies to trace the history of compliance with aviation rules, investigate events, and penalize violators. This includes not only the increased communication and coordination capabilities (Mehta et al. 2020; Gai et al. 2021) of UAVs and air traffic control authorities demanded by regulatory authorities but also the inclusion of other stakeholders, such as infrastructure operators, emergency responders, and urban planners into the management of smart city airspace. As such, for example, urban planners will need to exploit blockchain-based systems toward the optimal use of land and urban infrastructure to support UAV operations safely and efficiently. It is in this scenario that blockchain may be enabled on UAV communication systems, aid emergency responders in disaster responses, and coordinate on-the-fly data exchange for real-time situational awareness data collection. With its decentralized peer-to-peer coordination and communication capabilities among stakeholders, blockchain technology can drastically change UAV traffic control in smart cities. The complete urban air mobility in smart city airspace could ensure both safety and security through blockchain: a transparent, safe, and unhackable platform for data sharing and smart contract execution.

8.3 A Model for Adaptive Routing and Navigation Using Machine Learning and Blockchain

These agile UAV platforms offer previously never-imagined accessibility and agility in areas that were previously inaccessible, or at a location already crowded, where traditional methods turn out to be infeasible or ineffective. However, UAV integration into the smart city environment brings several challenges, mostly in routing and navigation. Indeed, operation under these scenarios is challenged because of complex infrastructure, high population density, and dynamic airspace legislation that characterizes modern urban scenarios. It requires sophisticated navigation systems capable of quickly adapting to changing situations, but it also requires effective, efficient, and safe movement of UAVs within such complications to strictly abide by safety and regulatory standards.

In light of these challenges, a framework is proposed to surmount these and finally realize UAVs to their full potential in smart cities. This model provides several innovative ways around the current constraints by integrating technologies like blockchain and machine learning with state-of-the-art UAV routing and navigation systems, as illustrated in Fig. 8.1.

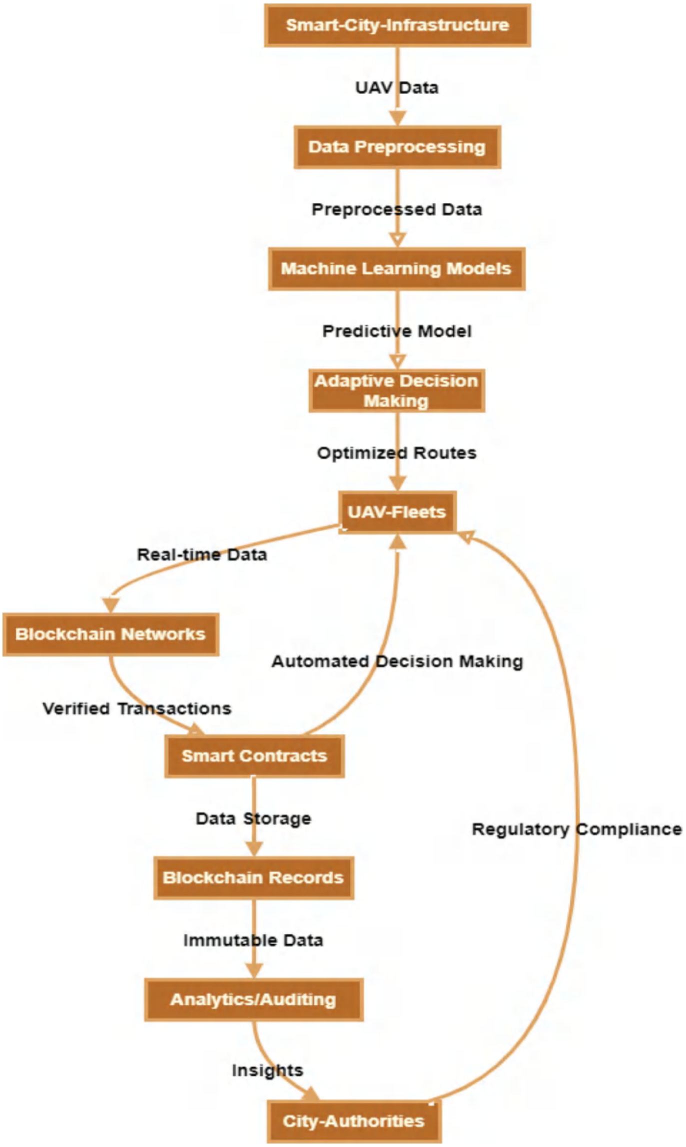


Fig. 8.1 A model for adaptive routing and navigation using machine learning and blockchain

Correctly, these optimizations will be majorly contributed by machine learning algorithms through the analysis of intricate data patterns and prediction of traffic dynamics in route adaptation for real-time usage by UAVs. The broad component overview within this framework is given below:

- Smart city infrastructure: Smart cities chain in real-time traffic patterns, weather, and other useful information about urban infrastructure through innumerable sensor networks, IoT devices, and data sources. Finally, it is in this context that these data sources might be very useful from the point of view they generate for new UAV navigation and routing, given their ability to realize fly route changes dynamically because of the change in urban conditions.

- Data Preprocessing: The raw data that would be obtained from these infrastructures in a smart city would be, in one way or another, pre-processed to bring out features and then transformed into a format suitable for input into machine learning models. This includes data cleaning, normalization, extraction of features, dimensionality reduction, and quality and efficiency assurance for the subsequent machine learning steps.
- Machine Learning Models: Many applications are developed from the training of machine learning models with the pre-processed inputs from UAVs; for instance, a supervised learning algorithm or a reinforcement learning approach can provide predictive optimal routes and navigation strategies. Such algorithms understand trends and come to very informed conclusions on the optimization of routes with the history of UAV flights, environmental conditions, and traffic patterns, among other contextual information. This method of navigation for UAVs can thus incorporate continuous learning and adaptation in terms of smarter and more efficient route selection by these algorithms, through iterative exploration of different routes and their performance evaluation by a defined objective, for example, maximization of energy efficiency or minimization of flight time.
- Adaptive Decision-Making: UAVs can dynamically replan their path based on the predictions that are generated using machine learning models to avoid traffic jams, inclement weather, and no-drone zones. The machine learning algorithms will allow the UAV to adapt its decision-making process to changing mission requirements and environmental factors. This way, decision tree algorithms, particle swarm optimization, genetic algorithms, and gray wolf optimization can classify different flight-related situations like construction zones and traffic accidents and provide recommendations for appropriate course changes or altitude adjustments.
- UAV Fleets: The UAV fleet includes UAVs equipped with onboard sensors, communication capabilities, and navigation equipment that fly routes determined by the decision-making function to be the most time- and cost-efficient. The UAVs work autonomously within the urban airspace on pre-defined navigation lines and change their direction based on real-time information and requests obtained from the system. In cases where several UAVs operate within the same restricted airspace, machine learning algorithms could be instrumental in making them very coordinated and cooperative to optimize system performance. Combining game theoretic methods, such as multi-agent reinforcement learning, can train tactics to learn coordination through interaction and negotiation among UAVs, highly improving the efficiency of aerial resource distribution and reducing conflict.

- Blockchain Networks: A decentralized, immutable blockchain network can be deployed to execute smart contracts over UAV operations and to record verifiable transactions. Since it is dependent on cryptographic linking and time-stamping, blockchain can prevent unwanted changes or tampering with the guarantee of integrity, transparency, and security in data.
- Smart Contracts: These are self-executing agreements whereby programs are placed on a blockchain and most of the specified criteria and rules for such agreements are in the code of the smart contract. They also automatize processes of decision-making and regulation enforcement, and allow transparent and auditable transactions between the operators of UAVs and the various authorities concerned, among other stakeholders, in the context of UAV routing and navigation.
- Blockchain Records: The Blockchain ledger provides visibility and verifiability to the trail of all system events by storing the tamper-proof record of UAV transactions, smart contract executions, and other relevant data storage. Data integrity is ensured by blockchain technologies, fostering stakeholder collaboration and data exchange with the ability to still be regulatory-compliant and accountable.
- Auditing/Analytics: Data analytics tools and auditing techniques will be used to analyze the blockchain data to derive valuable insights, for performance tracking within the system, and in ensuring all regulatory requirements are complied with. Similarly, such tools can provide meaningful feedback for the improvement of UAV routing and navigation algorithms as well as for the use in the amelioration of the general effectiveness of this system, solving new challenges in smart city scenarios.
- City Authorities: The city and regulatory authorities control all activities by UAVs operating in smart city environments. This aims to ensure that, by local laws and as laid down by airspace management guidelines and defined safety standards, UAV operations in urban areas are permitted. The city authorities are also working in association with private technology firms, UAV operators, and several other stakeholders to develop regulations, procedures, and guidelines for responsible and safe deployment and operations of UAVs in scenarios involving urban settings.

Moreover, even human-centric aspects can be integrated, including aspects of user preference or legal limitations and limits to safety, in the context of optimizing UAV routes in a smart city. Therefore, with the incorporation of data from social media, data from urban planning projects, and the preferences of the users, machine learning models could provide route recommendations capable of responding to personalized needs through course selection based on local regulation compliance and user enjoyment. Machine learning algorithms can go through this real-time data and historical data from sources such as traffic patterns, meteorological data, and urban infrastructure in the detection of trends and predictions on future circumstances. Machine learning models for predicting changes in traffic density, weather disruption, and other factors that may influence UAV navigation can be trained using techniques like regression analysis, time series analysis, and anomaly detection.

Through the integration of these components, a machine learning and blockchain-powered UAV routing and navigation system may improve safety and efficiency, optimize UAV operations, and facilitate the sustainable growth of smart cities. This framework can be customized according to applications, for example, the machine learning models can be included in blockchain networks. Table 8.1 lists some of the recent research concerning UAV routing involving heuristics, optimization, and blockchain-based/machine learning-based techniques with diverse applications.

8.4 Overcoming Challenges in Integrating Blockchain and Machine Learning with UAV Navigation Networks

A promising yet difficult frontier in smart city infrastructure development gives the integration of blockchain technology with navigation networks of UAVs. Since UAV usage is highly relevant to such fields as emergency response, delivery services, and surveillance, ensuring safe and effective functioning for such unmanned aerial vehicles is of high importance. In this regard, a decentralized and immutable nature makes blockchain a potential solution for enhancing efficiency, security, and dependability in UAV networks. However, to fully realize that integration, some challenges have to be overcome.

8.4.1 Complications and Prospective Solutions in Blockchain-Based UAV Routing and Navigation

There are many obstacles to overcome when integrating UAV routing and navigation with blockchain technology (Othman and Indiran 2023), and creative solutions are needed to guarantee dependable, secure, and effective operations in smart city settings. An elucidation of these issues and possible fixes is provided below:

8.4.1.1 Real-Time Data Manipulation

For UAV routing and navigation systems to make wise flight route decisions, avoid obstructions, and guarantee safe operation in smart city environments, they depend on fast and reliable data. However, consensus algorithms and transaction validation methods have inherent latency and scalability limits, standard blockchain networks might find it difficult to fulfill the real-time processing requirements of UAV operations.

Solutions:

- By parallelizing work among blockchain nodes (Bragagnolo et al. 2019), distributed computing approaches help reduce latency in UAV navigation decisions. These techniques improve real-time processing, which is essential for quick

Table 8.1 Show key aspects of the recent papers involving UAV routing/navigation systems with blockchain or machine learning models or both

	About	Limitations
2024		
Wang et al. 2024)	To continuously interact with external data, APPA-3D employs an anti-collision control method based on the UAV's ambient awareness. It optimizes path planning by combining reinforcement learning (RL) with a dynamic reward function, improving UAVs' capacity to avoid obstructions and arrive at targets without incident	
Saifullah et al. 2024)	In UAV ad hoc networks, K-means online learning routing protocol (KMORP) makes use of a 3D Gauss Markov mobility model for precise UAV position estimation and K-means online learning for load balancing and dynamic clustering	In dynamic/dense UAV networks: sensitive to the first cluster and outliers, overhead in cluster formation, management, and intercluster communication
2023		
Ramasamy et al. 2023)	Using a vehicle routing problem formulation that takes capacity limitations, time windows, and dropped visits into account, the UAV route is optimized	More complicated when the route is parameterized to take visiting sites and UAV recharging wait periods into consideration
Dong, et al. 2023)	Decentralized FL framework for edge-based smart UAV delivery systems based on blockchain technology. Uses a decentralized blockchain to store private information and a personalized proof of quality factor consensus procedure to guarantee accuracy/consistency	Single-point-of-failure in FL, scalability problem in the increase of intelligent applications
Yang et al. 2023)	BC-UTSON, a blockchain-driven UAV networking system designed to improve internal security. real-time full-node trustworthiness evaluation to increase system trustworthiness, U-PBFT for lightweight consensus, and BC-UTSON for self-organizing networking	Issues on dynamic topography, scarce resources and sensitive to internal hostile UAV assaults
Akter et al. 2023)	IoMT-Net is designed to track and identify illicit UAVs operating within the Internet of Military Things system. Combines blockchain technology with lightweight CNN model to produce accurate direction of arrival estimation for UAV identification	Issues include data manipulation, fabrication, and unauthorized access, problems when untrusted parties misuse UAVs
Cash et al. 2023)	Integrates a machine learning model to improve the B.A.T.M.A.N. routing protocol	No history of route conditions to incorporate

(continued)

Table 8.1 (continued)

	About	Limitations
Wang et al. 2023)	A flexible UAV swarm routing system that compresses communication data to increase efficiency and uses a gate recurrent unit to identify when routing flooding is necessary	Conventional methods for flooding searches result in significant overheads in communication and poor routing efficiency with greedy search
Dixit and Kumar Singh 2023)	Combining PSO, GA, and GWO, the BMUDF hybrid model enhances UAV routing by addressing issues such as computational complexity and poor performance in large-scale networks. Optimizing routes according to node locations, energy levels, throughput, and packet delivery, improves QoS	The precision of fault detection and the model's applicability to various UAV network settings are not answered
2022		
Yakimenko et al. 2022)	Blockchain-assisted path optimization system that uses smart contracts for gas limit allocation and device registration to combat security attacks and provide a safe path for UAVs to travel. Explores techniques for path planning in dynamic environments. RUPOA enhances path planning security and efficiency by integrating energy rate and authentication elements. It efficiently lessens security threats by keeping a routing table up to date, which shortens the communication gap between nodes	Restricted capacity to deal with ambiguous circumstances, susceptible to attacks using command/ control. The computational and communication overhead associated with a growing UAV fleet may increase, hence affecting the algorithm's performance and efficiency
Akram et al. 2023)	A new verified key agreement blockchain mechanism for UAV networks to improve security across a range of applications	
Huang, et al. 2022)	Trains the collision avoidance policy with depth image representations using an autoencoder and a policy gradient-based RL to ensure completely autonomous collision-free navigation in 3D	
Wang et al. 2022)	D3QN algorithm to learn decision-making strategies for UAV navigation without prior environment knowledge. Path-planning optimization to gather data from different nodes on its own	No exchange of data/ communication between UAVs
Kong et al. 2022)	Lightweight storage blockchain two-stage consensus procedure for UAV network management. Uses methods such as fuzzy K-modes clustering to achieve consensus. Allows dynamic and flexible trusted network building	Due to complexity and mobility, there is a risk of corruption, hijacking, and compromise

(continued)

Table 8.1 (continued)

	About	Limitations
Santos et al. 2022)	A machine learning model for UAV navigation in a satellite-less environment. Improved navigational accuracy and decreased noise sensitivity at the same execution time as the generalized trust region sub-problem technique	Reduced sensitivity to noise and decreased possibility of colliding with obstacles

navigation and obstacle avoidance in smart cities, by splitting and dividing computations. By optimizing blockchain networks for dynamic UAV operations, our method preserves distributed ledger system integrity while guaranteeing prompt and informed decision-making.

- Off-chain processing: This includes the outsourcing of time-critical computations from the blockchain into nearby or onboard computing resources, such as navigation-related calculations (Eberhardt and Tai 2017). This strategy makes UAVs more responsive by freeing them from blockchain consensus to enable real-time decision-making. In this way, with the use of edge computing devices or onboard systems, critical navigation computations could be executed locally, eliminating latency and thus responding quickly to changes in the environment. Therefore, off-chain processing ensures that the security and integrity of the data recorded on the blockchain are retained, while the UAVs autonomously provide navigation capabilities in smart city environments.
- Hybrid architectures partition computational load between off-chain processing and on-chain capture to drive back data integrity against real-time performance (Miyachi and Mackey 2021). More computationally resource-intensive operations take place off-chain, often using distributed or edge computing, while only light transactions are written to the blockchain. This retains the security and transparency given by blockchain technology while accessibly optimizing blockchain load and delay for mission-critical choices made in the course of UAV navigation.
- Optimizing data structures with compression techniques reduces the volume and complexity of UAV navigation data stored on the blockchain. In this regard, transaction throughput is improved as delay is reduced. Blockchain networks provide higher responsiveness for real-time updates. This represents data more effectively and hence is thus imperative for dynamic UAV routing and navigation in smart cities. This finally makes aerial navigation through urban environments safer and more effective by ensuring that blockchain-based systems can handle the demands of UAV operations while maintaining data integrity and decentralization.
- Low-latency consensus algorithms designed for real-time applications can be utilized. Such techniques, which prioritize the speed of validation of a transaction and reduce delays in processing, include directed acyclic graphs (Zhao and Yu 2019; Schett and Danezis 2021) and byzantine fault tolerance (Peng et al. 2024). In this regard, blockchain networks that support UAV operations can improve responsiveness to ensure updates related to flight paths and navigation instructions

are timely, therefore improving overall system performance in the dynamic smart city environment. This is ensured through the selection or design of consensus mechanisms optimized for quick decision-making.

It can be summed up that blockchain-based routing and navigation systems of unmanned aerial vehicles may, in real-time, deal with smart city-related data, thereby solving the mentioned challenges by applying distributed computing techniques, off-chain processing tactics, and optimized approaches to data management. These solutions leverage the security and transparency features of blockchain technology to realize autonomy in decision-making in UAVs.

8.4.1.2 Scalability

Blockchain scalability refers to a blockchain network's ability to handle an increased load of transactions or data without a decrease in effectiveness or performance. The following variables make this difficulty especially pertinent to integration:

- The systems for routing and navigation of UAVs generate a great deal of data and have to be updated frequently because of traffic patterns, environmental conditions, and changes in mission goals. Storing and processing this data on a blockchain network could cause congestion and poor performance, specifically during peak load conditions.
- Low transaction throughput, usually measured in TPS, of traditional blockchain networks, like Ethereum and Bitcoin. With an increasing number of UAVs and smart city apps, it could turn out to be emerging complex and time-consuming for the blockchain network to process the transactions quickly; this would bring about further delays and a higher transaction cost.

Solutions:

- Sharding (Hashim et al. 2023; Zamani et al. 2018) refers to the division of the blockchain network into more manageable, smaller portions called shards. It is, thus, a scalability solution. Every shard handles a portion of transactions individually for parallel processing and higher throughput. In this regard, blockchain networks are capable of enhancing transaction throughput without affecting security and decentralization simply by adding sharding.
- Although independent in themselves, sidechains are independent blockchain networks that can communicate with the main blockchain. In this respect, they can be employed to store data regarding UAV routing and navigation and analyze it for the same purpose of reducing the load from the primary blockchain network. Sidechains (Singh et al. 2020) can implement different consensus processes or optimization strategies for the unique needs of UAV operations.
- Off-chain transactions (Eberhardt and Tai 2017) get settled on the main blockchain only when necessary. These are enabled by layer 2 protocols like state channels and payment channels. UAV navigation systems can complete the bulk of the transactions of the chain using layer 2 protocols and thereby reduce congestion

on the main blockchain network, increasing scalability. Moreover, layer 2 protocols can reduce transaction costs for UAV operators and offer instant finality for transactions.

- Bring down the number of blockchain transactions required for navigation updates by UAV routing algorithm optimization. Again, any minor change in mission parameters or the flight path does not need to be recorded on the blockchain, as UAVs may locally aggregate this information and, once in a while, work out updates that it will publish to the blockchain network at a higher time quantum. By slashing the rate for blockchain transactions, the scalability issues can be resolved and overall efficiency enhanced by the UAV routing system.
- Design a hybrid blockchain architecture that puts together the various scaling techniques (Thibault et al. 2022; Hafid et al. 2020) to achieve better scalability and performance for UAV routing and navigation systems. Hybrid blockchain networks ensure high transaction throughput, low latency, and robust security by harnessing the benefits of each technique to assure reliable operation in smart city environments.

These solutions can, therefore, help drive new opportunities for effective and decentralized UAV operations in the context of smart cities by making seamless integration between blockchain technology and UAV routing and navigation systems possible, which long suffered from a scalability issue.

8.4.1.3 Privacy and Security

Coupling blockchain technology with UAV routing and navigation raises several serious privacy/security issues. For example, how to ensure private information, such as mission objectives, routes taken, or surveillance video, cannot cause others to view private activities or modify the data. These are only some instances. The following points expand the problem description on many solution possibilities:

- Privacy-sensitive information in UAV navigation data has to be protected from unauthorized access. Maintaining the integrity of UAV navigation data captured on the blockchain.
- Open UAV activities contrasted with the expectation of full privacy of private information, hence the need to navigate between the two.
- Access control to UAV navigation data by not allowing unfettered view ability and updatability of private data by unauthorized persons.
- Secure channels of information flows, which cannot be eavesdropped or interfered with, have to be there between the blockchain nodes and UAVs.

Solutions:

- End-to-end encryption assures data confidentiality of UAV navigation data since the data is already encrypted before it gets stored in the blockchain (Das et al. 2021). This does not allow any form of unauthorized access to their sensitive data, such as routes for the aircraft and mission details. In this view, secure and private anonymized UAV operations in smart city settings will be realized because entities provided with the decryption keys are the ones that can decode and thus have access to such information. Secondly, strong symmetric and asymmetric key-based cryptographic algorithms alongside secure key generation, distribution, and management techniques protect the UAV navigation data from every type of threat and breach.

- Digital signatures (Buchmann et al. 2009) would work to ensure integrity and authenticity, including cryptographic hash functions (Cid 2006) for UAV navigation data. Information is hashed into a special fingerprint that has to be stored on a blockchain. Later, this hash has to be digitally signed using a private key. Any party will be able to hash the data on their own with the hash function and compare it to the stored hash, then verify the digital signature using the public key, which will prove integrity. This will better maintain the data authenticity and integrity on board for UAV navigation, hence a much more reliable smart city application.
- Apply privacy-preserving mechanisms for verifying the validity using ring signatures or zero-knowledge proofs without revealing private information to any party other than the operator of the UAV. Zero-knowledge proof ensures the privacy and integrity of the data in transactions Ring signatures (Buchanan et al. 2023; Devidas et al. 2023), on the other hand, allow signing a message with a set without revealing which one of the members of the group is the signer. It allows safe checking of the UAV navigation data on the blockchain among operators without leaking operational-activity information and revealing dangerous or restricted areas.
- Access control mechanisms and permissioned blockchain networks make certain that sensitive UAV navigation data is accessed only by an authorized entity. There is access granted to information within smart contracts, which only allows data to be available to the caller according to pre-defined position roles and permissions assigned to the position. In this way, the chance that data could be accessed or manipulated without permission decreases to near zero.
- Secure communication channels from UAVs and blockchain nodes help to avoid both data tampering and data interception. Dependable protocols like DTLS or TLS have to be used for the data being communicated and correspondingly avail confidentiality/integrity. Use safe authentication, at least cryptographic keys, and digital certificates to ensure the communication endpoint identities with the least chance of data tampering or other unwarranted access. It enhances the overall security of the blockchain-enabled UAV systems in the smart city environment through the nourishment of confidentiality and integrity in the UAV navigation data.

8.4.1.4 Interoperability/Standardization

It would therefore take the seamless integration of data and interoperability among the different stakeholders in the ecosystem. Interoperability (Villarreal et al. 2023; Anthony 2024) can be hampered in that respect due to the lack of clear protocols and interfaces. This might result in silo types of systems that are pretty hard to integrate and scale. Besides, multiple stakeholders may have different requirements and preferences, which actually might escalate the problem with interoperability. Some of the stakeholders include data handlers, regulatory bodies, UAV manufacturers, and blockchain platforms.

Solutions:

- The establishment of one common set of standards/protocols with key industry players, standard organizations, and regulatory agencies concerning blockchain integration, data formats, and communication interfaces of UAVs. At a minimum, these standards should address the following key elements so that different UAV and blockchain systems can be compatible and interoperable in terms of network connectivity and message authentication and encoding.
- Designing interoperable frameworks/open-source reference implementations of the best practices about implementing blockchain technology in UAV routing and navigation systems. Such frameworks will provide practical guidance to solution providers, thus demonstrating best practices for the integration of UAV routing and navigation using blockchain. In that manner, the codes and methodologies shall be shared freely within the community to jointly work together and develop standardized procedures along with efficient integration processes. Its creativity improvement is toward a situation whereby wider sets of stakeholders can have access to interoperable solutions, hence gradually contributing to UAV and blockchain technologies in smart city scenarios.
- Design modular designs/standardized interfaces for blockchain platforms and UAV routing and navigation systems that enable a plug-and-play integration approach. Commonly used data interchange formats and communication protocols appropriate for universal adoption are followed, hence enabling easy integration with third-party systems and existing infrastructure. This eventually paves the way for scalability and minimizes any difficulties in implementation by providing interoperability among components and enabling seamless data flow and communication across different components of the ecosystem.
- Pilot programs and testbeds to test interoperability solutions in concrete scenarios. Conducted through research centers, smart city partners, and industry associations, they offer a valuable view of the issues. By the testing, revision, and change of standards and protocols, according to the feedback from the big stakeholders in the area, it is made possible to create interoperable systems that work fine together.
- Interoperability standards and protocols to meet industry best practices and regulatory requirements for UAV operations and suitability for blockchain applications. Collaboration with regulatory bodies in building interoperability standards which encompass features to ensure regulatory compliance. An illustration is the recording of airspace limits and flying authorizations in the blockchain ledger.
- Proper considerations of the challenges of interoperability/standardization in combining blockchain technology with UAV routing and navigation systems

in smart city applications can, however, be effectively remedied with stakeholder actions in the way of industry collaboration, open standards, and regulatory alignment (Anthony 2024). Such interoperability allows for the seamless sharing of information, data interchange, and collaboration in various UAV and blockchain ecosystems, opening innovative and scalable solutions in public safety, infrastructure management, and urban mobility.

8.4.1.5 Regulatory Compliance

One of the most important aspects of UAV operation is regulatory compliance, considering it more in the urban setting where their airspace is heavily restricted. Compliance involves adhering to the myriad of rules that have so far been put in place by regulatory bodies, municipalities, and authorities charged with air space governance (Akanfe et al. 2024; Buterin et al. 2024; Jia et al. 2024). Applying blockchain technology to ensure compliance raises several concerns.

- The operation of UAVs is surrounded by many laws concerning areas such as pilot licensing, airspace restrictions, flying authorization, and also privacy issues. These regulations are tedious and time-consuming to go through and ensure they are complied with accordingly.
- Ensure safety and security, requires some level of responsibility and transparency concerning the UAV operations to regulatory organizations. Traditional models of paper-based or centralized systems lack transparency and thus it becomes minimally effective to enforce standards and successfully verify compliance.
- UAV activities often involve crossing borders, and thus conformance to the laws of multiple authorities is required. UAV operations become significantly complicated while trying to conform to many regulatory provisions—especially in smart city use cases where airspace may be shared by many different stakeholders.

Solutions:

- Blockchain technology will establish a tamper-proof, immutable record-keeping database for UAV operations—inclusive of pilot credentials, flying permits, airspace limits, and other regulatory data. This open record-keeping would give way to compliance with rules and thus offer the possibility of effective auditing of UAV operations by regulatory bodies.
- Smart contracting can be implemented on a blockchain to achieve automation in compliance. As an example, self-executing contacts bear the power to enact legislation regarding airspace compliance, no-fly areas, and prescribed limitations on aircraft with respect to altitude. All breaches regarding rules may be met with automatic fines or notification given to the relevant regulatory authorities.
- Blockchain allows verification and authorization of activities to be carried out in a decentralized manner. This eliminates the regulatory bodies from having to centrally authorize every single flight manually. There is brought about transparency and efficiency since the authorized parties like the regulatory bodies can

get to see the Blockchain ledger to confirm whether UAV operations are within compliance or not.

- Market blockchain platforms may be designed to integrate and interface with the legacy databases and regulatory systems to enable easy integration and interchange of data. Blockchain-based UAV systems and regulatory/statutory repositories may communicate with one another to enforce regulatory reporting standards, using APIs and standardized data formats.
- There are at least two privacy-enhancing technologies—selective disclosure of techniques and zero-knowledge proofs—into which blockchain can be applied so that blockchain regulatory bodies can verify for compliance without ever having had access to sensitive data. This would provide for regulatory control but secrecy over sensitive data, like flight logs or personally identifiable information.

It can also enhance the efficiency, transparency, and compliance related to regulations regarding a smart city setting by making use of blockchain technology to resolve issues that come with regulatory compliance for UAV operators. The solutions to be developed to ensure compliance with the regime in UAV operations have to use blockchain-based technology and collaborate with industry partners, regulators, and technology companies in its development and implementation.

8.4.1.6 Energy Efficiency

Usually, only limited onboard power sources are available with UAVs (e.g., batteries); hence, flying time and load ability are directly related to and therefore limited by the onboard power availability. In particular, considering blockchain technology's integration, this could further increase the problems of energy consumption due to the often computationally intensive consensus techniques involved (like proof of work) (Lin 2023), thus reducing the already reduced applicability of blockchain-enabled UAV applications in smart cities even more.

Solutions:

- Proof of stake (Tang et al. 2023) does not result in energy-guzzling mining. Here, a person's stake in the cryptocurrency forms the basis of choosing the validators. A nexus of good behavior is promoted and illegal behavior is discouraged as the validators stake their coins in the process. When blockchain networks transit from the Proof-of-Work (PoW) systems to Proof-of-Stake (PoS) systems, they become "greener". Thus, they can suitably serve the UAV applications in smart city scenarios. In routing and navigation systems, this energy-efficient approach would ensure that flight endurance and operational efficiency of the UAV are not affected by integration with blockchain operations.
- Proof of Authority (PoA) (Nazir, et al. 2023; Maftei et al. 2023) does not require energy-intensive mining and needs only a few validators to be able to validate transactions and build blocks. Within the blockchain systems supporting UAV operations, PoA saves a lot of energy usage with pre-defined authority that guarantees the integrity of the network. Finally, this methodology also enables the use of

blockchain-powered UAV application deployments that are more energy-efficient routes and navigation in smart cities and allow for longer flight times.

- Directed Acyclic Graphs (DAGs) (Zhao and Yu 2019; Schett and Danezis 2021) are a potential solution to merge blockchain with UAV in a power-efficient manner. In DAG-based consensus algorithms, like Tangle in the IOTA, there is no mining or generation of blocks as in traditional blockchains. Such a graph structure keeps the transactions interlinked with fewer resource-intensive computations. DAGs remove burdens associated with traditional consensus techniques, so that, in smart city scenarios, UAVs can directly talk to the blockchain and validate transactions in a decentralized and secure manner, not wasting precious onboard energy on less-important tasks.
- Computational tasks related to blockchain offloaded from UAVs to the ground-based nodes or cloud infrastructure. This greatly reduces the energy load on UAVs, freeing their limited onboard power for key flight operations. Offloading some of these non-essential duties to nearby computer resources would not make UAVs compromise operational efficiency. These offloaded duties, including consensus procedures and transaction validation, take place away from the UAVs to make more critical flight operations feasible. Such an approach warrants prompt and responsive UAV operations in smart city settings by decreasing latency in blockchain transactions and increasing energy efficiency. Offloading computational chores to nodes in the ledger-keeping network also enhances scalability, thus helping to meet the growing requirements of blockchain-enabled UAV applications by distributing the computational burden.
- In developing countries, UAV flight paths and mission priorities will have to be adjusted accordingly based on the current state of the blockchain network and available energy reserves. In this regard, a UAV, through continual monitoring of variables such as battery life, network load, and processing time for each type of transaction, can adjust its operations to reduce its overall energy consumption while maintaining efficient blockchain communication. This dynamic resource allocation approach allows UAVs to enable real-time adaptive behavior, allowing them to make dynamic priority settings of activities in case of high network traffic or a shortage of resources with less energy consumption. In addition, with the use of machine learning and predictive analytics, dynamic resource allocation algorithms will be able to forecast future energy demand and adjust trajectories accordingly. In smart city environments, unto quản UAVs can achieve optimal operating efficiency and endurance in smart city environments by effectively managing resources and optimizing mission planning.
- In UAV systems draped by blockchain technology, dynamic resource allocation algorithms (Liu et al. 2024; Xu et al. 2024) offer effective energy utilization and workload management. These algorithms focus on real-time optimization of the flight paths and task scheduling of UAVs through the continuous reassessment of variables such as available energy reserves, network conditions, and mission priority. It could also be used by UAVs to change the trajectory of a flight dynamically for resource sharing, considering varying environmental conditions

and blockchain network demands, to achieve minimal energy consumption and maximal operational efficiency.

8.4.2 Issues in Developing Machine Learning-Driven UAV Navigation Systems

Several issues of environmental influence, urban dynamics, and real-time data processing arise, which must be addressed to design a machine learning-driven UAV navigation system (Peng et al. 2023; Xue and Chen 2023; Prasad et al. 2023; Braathen De Carvalho et al. 2023) over the smart city. These are explained as follows.

8.4.2.1 Constraints in UAV Real-Data Processing

UAVs are embedded with onboard sensors (Osco et al. 2021) like GPS, LiDAR, and cameras, outputting huge amounts of generated data in real time. Fast navigation decisions require efficient processing of the generated data.

- The computational resources of UAVs are usually restricted with respect to computing power, memory, and energy. Processing constraints in these dimensions often exacerbate the difficulty of executing machine learning tasks in real time.
- The requirements of real-time processing demand low latency algorithms that can make navigation move quickly—very often within milliseconds or microseconds.

Solutions:

- Lightweight, resource-constrained machine learning algorithms are used many times by developers to circumvent processing limitations.
- Techniques such as quantization, pruning, and compression of models reduce computational and memory requirements for a machine learning model while it is still performing satisfactorily. For instance, binary or ternary neural networks use fewer bits to encode weights, significantly bringing down the memory and computational cost of inference on a UAV.
- Hardware acceleration technologies, like GPUs and FPGAs, can be applied to UAVs to realize enhanced real-time processing. These hardware accelerators let UAVs finish intricate inference tasks more expediently by allowing better execution of machine learning computations, thus cutting energy usage. Further improvement in performance and efficiency can be realized by running machine learning algorithms using libraries and frameworks optimized for specific hardware platforms.
- Onboard computing refers to the technique whereby onboard computational resources on the UAV are used for processing and analysis directly on the aircraft.

- Edge computing involves an expansion of the above idea where the processing duties are split between edge devices on the network, including base stations or ground control stations. Workload offloading to onboard or edge computing platforms can reduce latency and bandwidth requirements in a UAV for connection to remote servers as the computation-intensive jobs will now reside on these devices. This will enable faster decision-making in real-time situations.
- Real-time processing will call for the design of efficient data pipelines. Here, one will need to set priorities for relevant computations, eliminate redundancy and mobility in data, and optimize input/output of data. They can make the pipelines of data more efficient. Batching, asynchronous processing, and data streaming strategies could make a huge difference in reducing the processing overhead of a data pipeline.
- The strategy of optimizing algorithms to low computational complexity/small memory footprint can further improve real-time performance for these resource-constrained UAV platforms.

By this means, integrating these approaches can help the developers overcome the processing of data in real time, and the UAVs can efficiently perform high-level machine learning tasks (Osco et al. 2021; Barik et al. 2022; Kumar 2024; Kurunathan et al. 2024) in smart city environments. Hence, more reliable operation of UAV systems with better overall performance makes navigation easier and faster.

8.4.2.2 Environmental Factors

Any empowered machine learning UAV navigation system for smart cities must not sideline consideration for environmental factors, especially erratic weather conditions (Han et al. 2023; Wilson et al. 2022; Eskandari et al. 2020). Some examples of environmental factors that might impact UAV navigation include weather, topography, and obstructions.

- The nature of weather like wind direction and speed, precipitation, fog, and temperature may affect the functioning@@@@ of sensors used in UAVs and the dynamics of flying.
- Buildings, trees, mountains, bodies of water, etc.—these are some of the very different landscape components that cause trouble for UAV navigation and obstacle avoidance. Buildings, power lines, bridges, moving cars, humans, and wild animals are some of the static and dynamic impediments that need to be detected and avoided during UAV operations.
- UAVs typically rely on onboard sensors, such as GPS, LiDAR, and cameras, for navigation. However, these are susceptible to bad weather conditions or other factors related to topography, which may result in poor performance or incorrect data.
- Urban scenes are very complex and comprise ordinarily a huge number of buildings, dynamic elements, and other static obstacles that UAVs need to fly safely around.

Solutions:

- Multi-sensor fusion—Information from cameras, LiDAR, GPS, and IMUs gives situational awareness to machine learning-driven UAV navigation. The framework provides resilience for navigation because the limitations and failures of the individual sensors are offset by redundancy. Algorithms align and synchronize a coherent image of the environment in which the UAV is flying. Effective approaches to the fusion of heterogeneous sensor data include sensor fusion networks and Kalman filtering. Many sensors can be utilized to allow UAVs to fly safely and successfully in smart cities by increasing the system's reliability and accuracy. Reliability and accuracy are very important in passing through complicated urban areas that include a variety of environmental conditions and barriers.
- Adaptive algorithms of machine learning-driven UAV navigation systems enable real-time adaptation to shifting environmental conditions without user intervention/retraining. Models (Jagannath et al. 2021; Sharma 2021) can still be improved continuously by the upcoming data using techniques including reinforcement learning and online learning. Besides, dynamic policy updates enable the UAV to adjust dynamically its navigation techniques with regard to environmental cues and mission objectives. Adaptive algorithms can provide a way for the UAV to navigate through dynamically changing smart city environments safely and effectively, making them more autonomous and responsive to real-world situations.
- Probabilistic modeling (Sharma 2021) for solving environmental problems. In this, uncertainty is being modeled through Gaussian processes and Bayesian inference. In developing probabilistic sensor fusion algorithms, noise and measurement errors are considered in elegantly integrating data from sensors; and through risk assessment of navigation, actions are well-informed judgments that balance efficiency with safety. The UAV performs real-time updates of environmental beliefs and state estimation through methods like Bayesian filtering. Probabilistic modeling under dynamic smart city contexts for navigation boosts robustness makes it more dependable, and assures efficient UAV operation under unpredictable circumstances.
- Solve environmental problems in machine learning using data augmentation (Ponnusamy and Natarajan 2021; Song et al. 2020). That is done by creating artificial datasets to imitate several aspects of the environment like geography and weather. Moreover, one also has the option of fine-tuning models with real sensor data using domain adaptation methods. Transfer learning uses information in one setting to improve performance in another. Artificially augmenting generated samples into the training data increases diversity. These techniques strengthen and make the UAV navigation systems resilient to actual situations, enhancing their powers toward safe and successful travel in the dynamic settings of smart cities.

- Hybrid techniques combine autonomous capabilities with human oversight and aim to improve safety and adaptability in a dynamic urban context. These technologies enable UAVs to be operated semi-autonomously, where human operators intervene or provide some form of direction when needed, while still allowing autonomous execution of navigation duties. Shared autonomy models demonstrate the fact that partial control authorities can be granted to both the human operators and the onboard UAV autonomy system with seamless handovers between autonomous and manual modes and cooperative decision-making. Hybrid approaches to resilient and successful navigation of complex smart city contexts make use of the complementary advantages of human expertise and autonomous navigation algorithms.

In this context, the latest approaches of machine learning and adaptive algorithms will help designers accommodate environmental constraints to offer UAV navigation systems capable of operating in dynamic Smart City environments while remaining resilient under highly varying circumstances.

8.4.2.3 City Dynamics

The urban environment is very dynamic and complex, with UAV navigation driven as a result of the population density, flow of traffic, and construction. Addressing urban dynamics in the context of machine learning-driven UAV navigation systems involves the obstacle of navigating through dynamic and complex urban environments (Prawiyogi et al. 2022; Abdalla and Marojevic 2020; Ullah et al. 2020).

- Reliable detection and tracking of dynamic objects in crowded urban scenarios eludes conventional computer vision algorithms, especially in challenging light and weather conditions.
- Finding the future motion of dynamic obstacles to avoid presumes the understanding of complex interaction patterns and the capacity to predict changes in motion paths.
- The development of provably safe, efficient, and law-abiding navigation algorithms that can cater to different urban environments.
- Real-time coordination of multiple UAV movements without collision and maximizing the system's performance is a difficult problem that appeals to techniques of negotiation and coordination for its solution.

Solution:

- Deep learning-based object detection/tracking methods permit robust detection/ tracking of dynamic obstacles within crowded urban landscapes. With the use of CNN models trained on various city datasets, UAVs can detect nearly every type of object and its motion patterns. It improves navigation safety and dependability in difficult or Hazardous circumstances. More to this, these algorithms could normally be included in the UAV navigation systems on account of improvements in real-time processing and sensor integration, whereby dynamic obstacles will be swiftly detected and tracked during a flight. It could be done by creating machine learning models estimating future trajectories in line with the previous motion data, such as LSTM/RNNs with long short-term memory/ recurrent neural networks. These may include context information to enrich and increase the accuracy of predictions, like pedestrian intention and traffic rules, and scene semantic information. Temporal dependencies are learned by these models, which provide the UAVs with the facility of predicting changes along their flight path, hence allowing proactive trajectory planning and collision avoidance in dynamic urban locales.

- Enabling UAVs to change navigational plans instantaneously by using reinforcement learning techniques. It is possible to dynamically adjust the routes and behaviors of a UAV for an urban setting by teaching an agent to optimize certain goals such as reducing travel time, maximizing safety, and complying with regulations.
- One big challenging effort toward multi-agent coordination and collaboration is the creation of distributed machine learning techniques (Dhuheir et al. 2023; Guo et al. 2022) that will allow UAVs to communicate, interchange data, and plan trajectories jointly. The coordination techniques are rendered efficient through strategies, such as coalition building, decentralized decision-making, and game theory, which ultimately enable autonomous UAVs to operate in an urban environment with safety and effectiveness.

These solutions will empower the machine learning-driven navigation systems of UAVs to become possible and cope with the complex and dynamic landscapes of smart cities, hence surmounting such obstacles linked with urban dynamics and ensuring safe and effective UAV operations in urban settings.

8.4.2.4 Integration/Fusion of Data

UAVs acquire information from several sensors, such as GPS, LiDAR, cameras, and IMUs. The navigation procedure is realized by data fusion from multiple heterogeneous sources (Alshaibani et al. 2022; Sultan et al. 2021; Ahmed et al. 2021)—precise information extracted from GPS, LiDAR, cameras, and inertial measurement units (IMUs) accurately.

- Sensor data acquired by UAVs may have noise in it due to many factors, such as signal interference, ambient disturbances, or even sensor errors. The output might vary due to environmental changes, variation of the sampling rate, or simply miscalibration.
- Whereas most sensors offer complementary information about the environment, their integration requires solving differences in data modalities, resolutions, and coordinate systems. This makes the integration of heterogeneous data challenging with regard to data format, scale, and unit differences.
- The inaccuracies in the measurements are inherent in the sensors because of things like sensor noise, changing ambient conditions, and low resolution. It is very important to model and propagate uncertainty efficiently through the fusion

process to achieve the right level of reliability in navigational decisions and the amount of trust in estimates provided by the UAV.

Solutions:

- Sensor biases and errors should be controlled using stringent calibration protocols to ensure precision, accuracy, and consistency of measurements. Online error correction algorithms and other methods based on sensor fusion calibration could be used to enhance the confidence level of sensor data. Besides, regular recalibration procedures are recommended to maintain the effectiveness of calibration with time. This will prevent drift and ensure continued accuracy in UAV sensor data.
- Methods like data cleaning and alignment can be used to remove anomalies and artifacts from the sensor data to prepare it for fusion. In creating a common reference frame from data supplied by multiple sensors, alignment ensures consistency. Calibration parameters and coordinate transformation techniques aid alignment and facilitate the effective fusion of heterogeneous sensor data. This means that in UAV navigation systems driven by machine learning, preprocessing, and alignment accelerate the fusion process and enhance the quality and reliability of the fused data for visual tasks such as localization, mapping, and obstacle recognition.
- Distributed and parallel processing techniques shall form part of the strategies to be applied to meet the real-time processing demands that come with UAV navigation systems. In particular, massive volumes of sensor data are handled fast with minimal delay by distributed computing platforms, hardware acceleration, and multi-threading in unmanned aerial vehicles. All of these techniques allow the integration of sensor fusion algorithms with navigation systems to ensure a quick and correct navigation decision. Distributed and parallel processing techniques, therefore, play a very important role in making machine learning-driven UAVs have successful navigation and motion in dynamic smart city settings.
- Probabilistic fusion models use particle filtering, Kalman filtering, and Bayesian inference that include explicit representation and propagation of uncertainty through the fusion process. This will help decide on a confidence level where the predictions of machine learning-powered UAV navigation systems make dependable navigation decisions. It provides a probabilistic estimate of the UAV state in dynamic situations with possible noisy or inconsistent sensor data using probabilistic fusion models and enables reliable navigation.
- Applying machine learning approaches for feature extraction and fusion is also recommended. This is fused with information obtained by segregating informative elements from sensor data. Deep learning or other methods that extract relevant features from raw sensor data could be a very effective way to improve the resiliency and effectiveness of a fusion process. In this regard, feature extraction embedded in fusion algorithms can effectively exploit multiple sensors' data in UAVs. Hence, this improves the accuracy of perception and aids in making more informed navigation decisions in a smart city environment.

- Adaptive fusion strategies are capable of dynamic changes in their fusion parameters concerning considerations linked to environmental factors and data dependability. These solutions are characterized by feedback mechanisms in an effort toward changing the fusion algorithms online to ensure stability under changing contexts. In other words, adaptive fusion solutions attempt to achieve real-time optimization of the performance of fusions to enhance the precision and dependability of navigation systems for UAVs through constant monitoring of the dynamics of the environment surrounding the UAV and quality assessment of sensor data.
- This can be done by fusing the former with navigation algorithms to provide integrated, fused sensor data input into the decision-making process of UAV navigation systems. This kind of integration will drive real-time action through perception in closed-loop control. With the fusion of direct navigation algorithms, UAVs will make informed navigation decisions based on their surroundings. It, therefore, assures that the UAVs would adjust to the dynamics of the environment and fly autonomously with very high accuracy and efficiency in an extremely complicated scenario like an urban area.

The above solutions can help designers thereof develop reliable and effective methods for data combination and integration in machine-learning-based navigation systems in unmanned aerial vehicles. Equipped with these techniques, UAVs will sense their surroundings effectively, make informed navigational decisions, and thus navigate autonomously in complex and dynamic environments like smart cities.

8.5 Conclusion

This chapter has stressed the key potential of blockchain operations and its conjunction with machine learning and UAV navigation systems in smart cities. It contributes to how these technologies can advance UAV operations by looking at decentralized UAV traffic control systems and communication protocols, providing a framework to adapt routing and navigation. Although the prospect of blockchain technology and machine learning seems very bright, some challenges remain. Identities are compliance necessities—with concerns to privacy and safety—the challenges of collaboration, growth issues, and energy consumption. For us to enjoy the benefits of integrating blockchain and machine learning in UAV navigation networks, we have to surmount several obstacles. Further, the chapter articulates challenges and limitations in the development of machine learning-powered UAV navigation systems. The performance of machine learning algorithms for UAV navigation in dynamic city environments is influenced by many factors. Some are environmental, while others include changes at the city level, data joining issues, and processing real UAV data limits. To summarize, blockchain, machine learning and UAV navigation systems can quickly revolutionize smart city operations by simply collaborating and implementing these technologies. That is, this will be in sending strong, scalable systems that improve UAV routing, communication, and navigation in cities, so long as the challenges previously mentioned are addressed. Blockchain-powered UAV navigation systems will come to form cities that are safer, more mobile, and more sustainable in the future. This will be realized through ongoing research and development.

References

Abbas N, Abbas Z, Liu X, Khan SS, Foster ED, Larkin S (2023) A survey: future smart cities based on advance control of unmanned aerial vehicles (UAVs). Appl Sci 13(17):9881. https://doi.org/10.3390/APP13179881

Abdalla AS, Marojevic V (2020) Machine learning-assisted UAV operations with the UTM: requirements, challenges, and solutions. In: IEEE vehicular technology conference, vol 2020, November 2020. https://doi.org/10.1109/VTC2020-FALL49728.2020.9348605

Ahmed A, Ngoduy D, Adnan M, Baig MAU (2021) On the fundamental diagram and driving behavior modeling of heterogeneous traffic flow using UAV-based data. Transp Res Part A Policy Pract 148:100–115. https://doi.org/10.1016/J.TRA.2021.03.001

Akanfe O, Lawong D, Rao HR (2024) Blockchain technology and privacy regulation: reviewing frictions and synthesizing opportunities. Int J Inf Manag 76:102753. https://doi.org/10.1016/J.IJINFOMGT.2024.102753

Akram MA, Ahmad H, Mian AN, Jurcut AD, Kumari S (2023) Blockchain-based privacy-preserving authentication protocol for UAV networks. Comput Netw 224:109638. https://doi.org/10.1016/J.COMNET.2023.109638

Akter R, Golam M, Doan VS, Lee JM, Kim DS (2023) IoMT-net: blockchain-integrated unauthorized UAV localization using lightweight convolution neural network for internet of military things. IEEE Internet Things J 10(8):6634–6651. https://doi.org/10.1109/JIOT.2022.3176310

Alsalami OM, Yousefpoor E, Hosseinzadeh M, Lansky J (2024) A novel optimized link-state routing scheme with greedy and perimeter forwarding capability in flying ad hoc networks. Mathematics 12(7):1016. https://doi.org/10.3390/MATH12071016

Alshaibani WT, Shayea I, Caglar R, Din J, Daradkeh YI (2022) Mobility management of unmanned aerial vehicles in ultra-dense heterogeneous networks. Sensors 22(16):6013. https://doi.org/10.3390/S22166013

Andreou A, Mavromoustakis CX, Batalla JM, Markakis EK, Mastorakis G, Mumtaz S (2023) UAV trajectory optimisation in smart cities using modified a∗ algorithm combined with haversine and vincenty formulas. IEEE Trans Veh Technol 72(8):9757–9769. https://doi.org/10.1109/TVT.2023.3254604

Anthony Jr B (2024) Enabling interoperable distributed ledger technology with legacy platforms for enterprise digitalization. Enterp Inf Syst 18(1). https://doi.org/10.1080/17517575.2023.2255979

Barenji RV, Nejad MG (2022) Blockchain applications in UAV-towards aviation 4.0. Stud Syst Decis Control 372:411–430. https://doi.org/10.1007/978-3-030-75067-1_18

Barik PK, Shah S, Shah K, Modi A, Devisha H (2022) UAV-assisted surveillance using machine learning. In: PDGC 2022 - 2022 7th international conference on parallel, distributed and grid computing, pp 384–389. https://doi.org/10.1109/PDGC56933.2022.10053282

Braathen De Carvalho K, De Oliveira IRL, Brandao AS (2023) AV navigation in 3D urban environments with curriculum-based deep reinforcement learning. In: 2023 international conference on unmanned aircraft systems, ICUAS 2023, pp 1249–1255. https://doi.org/10.1109/ICUAS57906.2023.10156524

Bragagnolo S, Marra M, Polito G, Gonzalez Boix E (2019) Towards scalable blockchain analysis. In: Proceedings - 2019 IEEE/ACM 2nd international workshop on emerging trends in software engineering for blockchain, WETSEB 2019, pp 1–7, May 2019. https://doi.org/10.1109/WETSEB.2019.00007

Buchanan BW, Ahmad J, Munir A, Wang L, Peng C, Tan W (2023) Secure ring signature scheme for privacy-preserving blockchain. Entropy 25(9):1334. https://doi.org/10.3390/E25091334

Buchmann J, Dahmen E, Szydlo M (2009) Hash-based digital signature schemes. Post-Quantum Cryptogr 35–93. https://doi.org/10.1007/978-3-540-88702-7_3

Buterin V, Illum J, Nadler M, Schär F, Soleimani A (2024) Blockchain privacy and regulatory compliance: towards a practical equilibrium. Blockchain: Res Appl 5(1):100176. https://doi.org/10.1016/J.BCRA.2023.100176

Cash M, Murphy J, Wyglinski A (2023) WIP: federated learning for routing in swarm based distributed multi-hop networks. In: Proceedings – 2023 IEEE 24th international symposium on a world of wireless, mobile and multimedia networks, WoWMoM, pp 316–319, March 2023. https://doi.org/10.1109/WoWMoM57956.2023.00049

Chen J, Du C, Zhang Y, Han P, Wei W (2022) A Clustering-based coverage path planning method for autonomous heterogeneous UAVs. IEEE Trans Intell Transp Syst 23(12):25546–25556. https://doi.org/10.1109/TITS.2021.3066240

Cid C (2006) Recent developments in cryptographic hash functions: security implications and future directions. Inf Secur Tech Rep 11(2):100–107. https://doi.org/10.1016/J.ISTR.2006.03.007

Crann V, Amiri P, Knox S, Crowther W (2024) Decentralized deconfliction of aerial robots in high intensity traffic structures. J Field Robot 41:1541–1557. https://doi.org/10.1002/ROB.22340

Dai R, Fotedar S, Radmanesh M, Kumar M (2018) Quality-aware UAV coverage and path planning in geometrically complex environments. Ad Hoc Netw 73:95–105. https://doi.org/10.1016/J.ADHOC.2018.02.008

Das M, Tao X, Cheng JCP (2021) BIM security: a critical review and recommendations using encryption strategy and blockchain. Autom Constr 126:103682. https://doi.org/10.1016/J.AUTCON.2021.103682

Devidas S, Rekha NR, Subba Rao YV (2023) Identity verifiable ring signature scheme for privacy protection in blockchain. Int J Inf Technol (Singapore) 15(5):2559–2568. https://doi.org/10.1007/S41870-023-01282-Y/METRICS

Dhuheir MA, Baccour E, Erbad A, Al-Obaidi SS, Hamdi M (2023) Deep reinforcement learning for trajectory path planning and distributed inference in resource-constrained UAV swarms. IEEE Internet Things J 10(9):8185–8201. https://doi.org/10.1109/JIOT.2022.3231341

Dixit A, Kumar Singh S (2023) BMUDF: hybrid bio-inspired model for fault-aware UAV routing using destination-aware fan shaped clustering. Internet of Things 22:100790. https://doi.org/10.1016/J.IOT.2023.100790

Dong C et al (2023) BDFL: a blockchain-enabled FL framework for edge-based smart UAV delivery systems. In: ACM international conference proceeding series. https://doi.org/10.1145/3591365.3592948

Eberhardt J, Tai S (2017) On or off the blockchain? Insights on off-chaining computation and data. In: Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), vol 10465. LNCS, pp 3–15. https://doi.org/10.1007/978-3-319-67262-5_1/FIGURES/5

Eskandari R, Mahdianpari M, Mohammadimanesh F, Salehi B, Brisco B, Homayouni S (2020) Meta-analysis of unmanned aerial vehicle (UAV) imagery for agro-environmental monitoring using machine learning and statistical models. Remote Sens 12(21):3511. https://doi.org/10.3390/RS12213511

Evangeline S, Lenin A, Kumaravelu VB (2023) Blockchain system for secure and efficient UAV-to-vehicle communication in smart cities. Int J Electron Telecommun 69(1):133–138. https://doi.org/10.24425/IJET.2023.144342

Gai K, Wu Y, Zhu L, Choo KKR, Xiao B (2021) Blockchain-enabled trustworthy group communications in UAV networks. IEEE Trans Intell Transp Syst 22(7):4118–4130. https://doi.org/10.1109/TITS.2020.3015862

Garau Guzman J, Baeza VM (2023) Enhancing urban mobility through traffic management with UAVs and VLC technologies. Drones 8(1):7. https://doi.org/10.3390/DRONES8010007

Guo Y, Zhao R, Lai S, Fan L, Lei X, Karagiannidis GK (2022) Distributed machine learning for multiuser mobile edge computing systems. IEEE J Sel Top Signal Process 16(3):460–473. https://doi.org/10.1109/JSTSP.2022.3140660

Gurtu A, Johny J (2019) Potential of blockchain technology in supply chain management: a literature review. Int J Phys Distrib Logist Manag 49(9):881–900. https://doi.org/10.1108/IJPDLM-11-2018-0371/FULL/XML

Hafeez S et al (2023) Blockchain-assisted UAV communication systems: a comprehensive survey. IEEE Open J Veh Technol 4:558–580. https://doi.org/10.1109/OJVT.2023.3295208

Hafid A, Hafid AS, Samih M (2020) Scaling blockchains: a comprehensive survey. IEEE Access 8:125244–125262. https://doi.org/10.1109/ACCESS.2020.3007251

Hamissi A, Dhraief A (2023) A survey on the unmanned aircraft system traffic management. ACM Comput Surv 56(3). https://doi.org/10.1145/3617992

Hamissi A, Dhraief A, Sliman L (2023) On safety of decentralized unmanned aircraft system traffic management using blockchain. In: 2023 IEEE international conference on enabling technologies: infrastructure for collaborative enterprises (WETICE), December 2023, pp 1–6 (2023). https://doi.org/10.1109/WETICE57085.2023.10477843

Han W et al (2023) A survey of machine learning and deep learning in remote sensing of geological environment: challenges, advances, and opportunities. ISPRS J Photogramm Remote Sens 202:87–113. https://doi.org/10.1016/J.ISPRSJPRS.2023.05.032

Hashim F, Shuaib K, Zaki N (2023) Sharding for scalable blockchain networks. SN Comput Sci 4(1):1–17. https://doi.org/10.1007/S42979-022-01435-Z/METRICS

Huang H et al (2022) Vision-based distributed multi-UAV collision avoidance via deep reinforcement learning for navigation. In: IEEE international conference on intelligent robots and systems, vol 2022-October 2022, pp 13745–13752. https://doi.org/10.1109/IROS47612.2022.9981803

Jagannath J, Jagannath A, Furman S, Gwin T (2021) Deep learning and reinforcement learning for autonomous unmanned aerial systems: roadmap for theory to deployment. Stud Comput Intell 984:25–82. https://doi.org/10.1007/978-3-030-77939-9_2

Javaid S et al (2023) Communication and control in collaborative UAVs: recent advances and future trends. IEEE Trans Intell Transp Syst 24(6):5719–5739. https://doi.org/10.1109/TITS.2023.3248841

Jia W, Xie T, Wang B (2024) A privacy-preserving scheme with multi-level regulation compliance for blockchain. Sci Reports 14(1):1–14. https://doi.org/10.1038/s41598-023-50209-x

Keith A et al (2023) A blockchain-powered traffic management system for unmanned aerial vehicles. Appl Sci 13:10950. https://doi.org/10.3390/APP131910950

Kong L, Chen B, Hu F (2022) Blockchain-assisted adaptive reconfiguration method for trusted UAV network. Electronics 11(16):2549. https://doi.org/10.3390/ELECTRONICS11162549

Kumar A et al (2024) Revolutionizing modern networks: advances in AI, machine learning, and blockchain for quantum satellites and UAV-based communication, March 2023. https://arxiv.org/abs/2303.11753v1. Accessed 16 Apr 2024

Kurunathan H, Huang H, Li K, Ni W, Hossain E (2024) Machine learning-aided operations and communications of unmanned aerial vehicles: a contemporary survey. IEEE Commun Surv Tutor 26(1):496–533. https://doi.org/10.1109/COMST.2023.3312221

Lin S (2023) Proof of work vs. proof of stake in cryptocurrency. Highlights Sci Eng Technol 39:953–961. https://doi.org/10.54097/HSET.V39I.6683

Liu Y et al (2024) Lightweight blockchain-enabled secure data sharing in dynamic and resource-limited UAV networks. IEEE Netw 38:25–31. https://doi.org/10.1109/MNET.2024.3383237

Liu Y, He D, Obaidat MS, Kumar N, Khan MK, Raymond Choo KK (2020) Blockchain-based identity management systems: a review. J Netw Comput Appl 166:102731. https://doi.org/10.1016/J.JNCA.2020.102731

Maftei AA, Lavric A, Petrariu AI, Popa V (2023) Blockchain for internet of things: a consensus mechanism analysis. In: 13th international symposium on advanced topics in electrical engineering, ATEE 2023. https://doi.org/10.1109/ATEE58038.2023.10108211

Mehta P, Gupta R, Tanwar S (2020) Blockchain envisioned UAV networks: challenges, solutions, and comparisons. Comput Commun 151:518–538. https://doi.org/10.1016/J.COMCOM.2020.01.023

Mishra P, Singh G (2023) Unmanned aerial vehicles in sustainable smart cities. Sustain Smart Cities 221–238. https://doi.org/10.1007/978-3-031-33354-5_10

Miyachi K, Mackey TK (2021) HOCBS: a privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Inf Process Manag 58(3):102535. https://doi.org/10.1016/J.IPM.2021.102535

Nazir A et al (2023) An optimized concurrent proof of authority consensus protocol. In: Proceedings - 2023 IEEE international conference on software analysis, evolution and reengineering, SANER 2023, pp 874–877. https://doi.org/10.1109/SANER56733.2023.00105

Osco LP et al (2021) A review on deep learning in UAV remote sensing. Int J Appl Earth Obs Geoinf 102:102456. https://doi.org/10.1016/J.JAG.2021.102456

Othman M, Indiran L (2023) The challenges of blockchain in digital era. Int J Bus Technol Manag 5(2):335–340. https://doi.org/10.55057/ijbtm.2023.5.2.31

Peng J, Lv B, Zhang L, Lei L, Song X (2023) An improved DDPG algorithm for UAV navigation in large-scale complex environments. In: IEEE aerospace conference proceedings, vol 2023, March 2023. https://doi.org/10.1109/AERO55745.2023.10115997

Peng S, Liu Y, Chen J, He J, Wang Y (2024) Petrichor: an efficient consensus protocol leveraging DAG and sharding for asynchronous BFT. In: Communications in computer and information science, vol 1897. CCIS, pp 284–297. https://doi.org/10.1007/978-981-99-8104-5_21

Ponnusamy V, Natarajan S (2021) Precision agriculture using advanced technology of IoT, unmanned aerial vehicle, augmented reality, and machine learning. In: Internet of Things, pp 207–229. https://doi.org/10.1007/978-3-030-52624-5_14

Prasad R, Lee G, Choi J-Y, Shim J, Song NC, Choi S (2023) Data-driven target tracking methods of UAS/UAM in dynamic environment, January 2023. https://doi.org/10.2514/6.2023-2660

Prawiyogi AG et al (2022) Smart cities using machine learning and intelligent applications. Int Trans Artif Intell 1(1):102–116. https://doi.org/10.33050/ITALIC.V1I1.204

Ramasamy S et al (2023) Solving vehicle routing problem for unmanned heterogeneous vehicle systems using asynchronous multi-agent architecture (A-teams). In: 2023 international conference on unmanned aircraft systems, ICUAS 2023, pp 95–102. https://doi.org/10.1109/ICUAS57906.2023.10156585

Sachdeva H, Gupta S, Misra A, Chauhan K, Dave M (2023) Privacy and security improvement in UAV network using blockchain. Int J Commun Netw Distrib Syst 29(4):383–406. https://doi.org/10.1504/IJCNDS.2023.131736

Saifullah, Ren Z, Hussain K, Faheem M (2024) K-means online-learning routing protocol (K-MORP) for unmanned aerial vehicles (UAV) adhoc networks. Ad Hoc Netw 154:103354. https://doi.org/10.1016/J.ADHOC.2023.103354

Santos R, Matos-Carvalho JP, Tomic S, Beko M, Correia SD (2022) Applying deep neural networks to improve UAV navigation in satellite-less environments. In: Proceedings – 2022 international young engineers forum in electrical and computer engineering, YEF-ECE 2022, pp 63–68. https://doi.org/10.1109/YEF-ECE55092.2022.9850152

Schär F (2021) Decentralized finance: on blockchain- and smart contract-based financial markets. Fed Reserv Bank St Louis Rev 103(2):153–174. https://doi.org/10.20955/R.103.153-74

Schett MA, Danezis G (2021) Embedding a deterministic BFT protocol in a block DAG. In: Proceedings of the Annual ACM Symposium on Principles of Distributed Computing, pp 177–186, July 2021. https://doi.org/10.1145/3465084.3467930

Sharma I (2021) Evolution of unmanned aerial vehicles (UAVs) with machine learning. In: Proceedings of international conference on advances in technology, management and education, ICATME 2021, pp 25–30. https://doi.org/10.1109/ICATME50232.2021.9732774

Singh A, Click K, Parizi RM, Zhang Q, Dehghantanha A, Choo KKR (2020) Sidechain technologies in blockchain networks: an examination and state-of-the-art review. J Netw Comput Appl 149:102471. https://doi.org/10.1016/J.JNCA.2019.102471

Song C, Xu W, Wang Z, Yu S, Zeng P, Ju Z (2020) Analysis on the impact of data augmentation on target recognition for UAV-based transmission line inspection. Complexity, vol 2020. https://doi.org/10.1155/2020/3107450

Sultan L, Anjum M, Rehman M, Murawwat S, Kosar H (2021) Communication among heterogeneous unmanned aerial vehicles (UAVs): classification, trends, and analysis. IEEE Access 9:118815–118836. https://doi.org/10.1109/ACCESS.2021.3107479

Tang D, He P, Fan Z, Wang Y (2023) Pool competition and centralization in PoS blockchain network. Appl Econ 56:6564–6583. https://doi.org/10.1080/00036846.2023.2274311

Thibault LT, Sarry T, Hafid AS (2022) Blockchain scaling using rollups: a comprehensive survey. IEEE Access 10:93039–93054. https://doi.org/10.1109/ACCESS.2022.3200051

Truong VT, Le L, Niyato D (2023) Blockchain meets metaverse and digital asset management: a comprehensive survey. IEEE Access 11:26258–26288. https://doi.org/10.1109/ACCESS.2023.3257029

Ullah Z, Al-Turjman F, Mostarda L, Gagliardi R (2020) Applications of artificial intelligence and machine learning in smart cities. Comput Commun 154:313–323. https://doi.org/10.1016/J.COMCOM.2020.02.069

Vaithinathan KK, Parthiban L (2022) Data management and industries automatization using blockchain, AI, and IoT. In: The convergence of artificial intelligence and blockchain technologies: challenges and opportunities, January 2022, pp 43–68. https://doi.org/10.1142/9789811225079_0003

Vaithinathan KK, Pernabas JB (2022) Revolutionizing legal services with blockchain and artificial intelligence. In: Blockchain for IoT, October 2022, pp 127–153. https://doi.org/10.1201/9781003188247-7/REVOLUTIONIZING-LEGAL-SERVICES-BLOCKCHAIN-ARTIFICIAL-INTELLIGENCE-KRISHNA-KUMAR-VAITHINATHAN-JULIAN-BENADIT-PERNABAS

Villarreal ERD, Garcia-Alonso J, Moguel E, Alegria JAH (2023) Blockchain for healthcare management systems: a survey on interoperability and security. IEEE Access 11:5629–5652. https://doi.org/10.1109/ACCESS.2023.3236505

Wang X, Gursoy MC, Erpek T, Sagduyu YE (2022) Learning-based UAV path planning for data collection with integrated collision avoidance. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2022.3153585

Wang Z et al (2023) Learning to routing in UAV swarm network: a multi-agent reinforcement learning approach. IEEE Trans Veh Technol 72(5):6611–6624. https://doi.org/10.1109/TVT.2022.3232815

Wang J, Zhao Z, Qu J, Chen X (2024) APPA-3D: an autonomous 3D path planning algorithm for UAVs in unknown complex environments. Sci Reports 14(1):1–18. https://doi.org/10.1038/s41598-024-51286-2

Wilson AN, Kumar A, Jha A, Cenkeramaddi LR (2022) Embedded sensors, communication technologies, computing platforms and machine learning for UAVs: a review. IEEE Sens J 22(3):1807–1826. https://doi.org/10.1109/JSEN.2021.3139124

Xu R, Chang Z, Zhang X, Hamalainen T (2024) Blockchain-based resource trading in multi-UAV edge computing system. IEEE Internet Things J 11(12):21559–21573. https://doi.org/10.1109/JIOT.2024.3375918

Xue Y, Chen W (2023) A UAV navigation approach based on deep reinforcement learning in large cluttered 3D environments. IEEE Trans Veh Technol 72(3):3001–3014. https://doi.org/10.1109/TVT.2022.3218855

Yakimenko O, Dong X, Manikandan K, Sriramulu R (2022) Optimized path planning strategy to enhance security under swarm of unmanned aerial vehicles. Drones 6(11):336. https://doi.org/10.3390/DRONES6110336

Yang J, Liu X, Jiang X, Zhang Y, Chen S, He H (2023) Toward trusted unmanned aerial vehicle swarm networks: a blockchain-based approach. IEEE Veh Technol Mag 18(2):98–108. https://doi.org/10.1109/MVT.2023.3242834

Zamani M, Movahedi M, Raykova M (2018) RapidChain: scaling blockchain via full sharding. In: Proceedings of the ACM conference on computer and communications security, pp 931–948. https://doi.org/10.1145/3243734.3243853

Zhao L, Yu J (2019) Evaluating DAG-based blockchains for IoT. In: Proceedings - 2019 18th IEEE international conference on trust, security and privacy in computing and communications/13th IEEE international conference on big data science and engineering, TrustCom/BigDataSE 2019, vol 2019, January 2019, pp 507–513, August 2019. https://doi.org/10.1109/TRUSTCOM/BIGDATASE.2019.00074

Zhao S, Wang W, Li J, Huang S, Liu S, Lolli F (2023) Autonomous navigation of the UAV through deep reinforcement learning with sensor perception enhancement. Math Probl Eng. https://doi.org/10.1155/2023/3837615

Chapter 9
Smart Irrigation and Climate Resilience: Leveraging IoT and Blockchain for Sustainable Agriculture

C. Manimegalai, K. Swetha, and R. Thenmozhi

Abstract A crucial and fundamental asset for the supportability of food, life, and the climate is water. In India, agribusiness utilizes more than 85% of the nation's water assets. To fulfill the prerequisite for food, the agribusiness exchange faces challenges related to over-the-top climate and common modification. To fulfill the creating prerequisite for nourishment, the agribusiness trade faces challenges associated with over-the-top climate and natural alter. Internet of Things (IoT) and blockchain propels have been instrumental in settling these issues. This is accomplished by utilizing state-of-the-art craftsmanship headways and orchestrated contraptions all through the agricultural cycle, from plowing soil to gathering created yields and joining them with blockchain development to offer farmers speedy information persistently. The IoT system can unequivocally recognize and spread adequate water for crops persistently, counting moistness, precipitation, temperature, wind, and soil conditions. The gathered data makes a difference in choosing the best harvests to create and keep up with, and it engages farmers to make a brief move in the occasion that negative climate designs develop. Progressed data around soil watching and day-to-day meteorological circumstances is put absent utilizing blockchain advancement. On the other hand, an IoT contraption water crops according to the day's temperature and the soil makeup. These climate condition guesses, plant water supply, cautions to farmers around water availability, and field recognitions are absent on blockchain. To meet the world's prerequisite for food, ranchers can work on creating capability and practicality by looking at the states of the soil, water, and supplements.

Keywords Reclaimed water · Irrigation efficiency · Sustainable agriculture · Smart farming · Resource optimization · Remote sensing · Decentralized systems

C. Manimegalai · K. Swetha (✉) · R. Thenmozhi
Department of Computer Science and Engineering, IFET College of Engineering, Villupuram, India
e-mail: swethapk2004@gmail.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2025

K. Ahmad et al. (eds.), *Fostering Machine Learning and IoT for Blockchain Technology*, Transactions on Computer Systems and Networks,
https://doi.org/10.1007/978-981-96-4074-4_9

9.1 Introduction

Agriculture today faces a multitude of complex challenges that threaten its sustainability and productivity. Central among these are the impacts of climate change, which include unpredictable weather patterns, increased frequency of extreme events, and altered growing seasons. These changes disrupt traditional farming practices, reduce crop yields, and exacerbate pest and disease problems, making it difficult for farmers to maintain consistent production levels (Harvey et al. 2014).

Water scarcity is another critical issue, intensified by climate change. Agriculture is the largest consumer of freshwater globally, yet inefficient irrigation practices lead to significant water wastage. Traditional irrigation methods often result in overwatering or underwatering, negatively impacting crop health and depleting precious water resources. As freshwater becomes increasingly scarce, there is an urgent need to optimize water usage to ensure long-term agricultural sustainability (Rabadiya Kinjal et al. 2017).

The agricultural supply chain also faces challenges related to transparency, traceability, and efficiency. Conventional supply chains are often fragmented and opaque, making it difficult to trace the origin and journey of food products from farm to table. This lack of transparency can lead to issues such as food fraud, contamination, and inefficiencies that increase costs and reduce profitability for farmers. Furthermore, the absence of reliable data hampers efforts to implement effective sustainability measures and respond to market demands accurately (Tian 2016).

Smallholder farmers, who represent a significant portion of the global agricultural workforce, are particularly vulnerable. These farmers often lack access to advanced technologies and financial services, limiting their ability to adopt modern agricultural practices, access markets, and secure fair prices for their produce. The technological divide between large-scale and smallholder farmers exacerbates inequality and hinders overall agricultural development (Tripoli and Schmidhuber 2018).

Integrating advanced technologies such as the Internet of Things (IoT) and blockchain presents a potential solution to these challenges. IoT can revolutionize irrigation practices by enabling precise water management through real-time data on soil moisture, weather conditions, and crop health. This data-driven approach can significantly reduce water wastage and enhance crop yields, contributing to climate resilience.

Blockchain technology offers solutions to supply chain inefficiencies by providing a secure, transparent, and immutable ledger for recording transactions and data points. This technology can enhance traceability, prevent food fraud, and ensure compliance with sustainability standards. Additionally, blockchain can facilitate financial inclusion for farmers through smart contracts and decentralized finance (DeFi), offering better access to markets and resources (Kouhizadeh et al. 2020).

However, adopting these technologies in agriculture is hindered by several barriers, including high implementation costs, lack of technical expertise, and resistance to change among traditional farming communities. Technical challenges such as the interoperability of different IoT devices and blockchain platforms also need to be addressed to fully realize these technologies' benefits (Lin et al. 2018).

To offer assistance to specialists and pioneers in soil viable and flexible nourishment creation and utilization, as well as to advance create investigations, this paper settled fitting issues associated with (1) physical and economic water wastage in agriculture; (2) water-saving strategies and gadgets; (3) crop and field observation; (4) WF assessment strategies; and (5) Storing of information using IoT and Blockchain technology.

It will spare water, and it will offer the culminate extent of water to the plant brilliantly. Other than that, the system can offer irrefutable information and design examination, engaging clients to take after the turn of occasions and execution of plants unavoidably. It will be utilized to settle on conclusions approximately plant care and streamline resource designation to develop plant prosperity. A further plant-watching system with IoT is an essential and beneficial strategy for managing plants from removal. IoT development licenses farmers, landscapers, and plant sweethearts to create advancement techniques, effectiveness, and plant well-being.

9.2 Problem Statement

Despite being necessary for human survival and the stability of conditions, freshwater is the resource that is most exploited globally. Overuse of freshwater, which occurs when the interest in freshwater exceeds its resource, can result in a shortage in the dispersal rate. Water utilization in all human endeavors ought to progress, taking into account the deficiency of freshwater coming approximately since natural alter and the 81,000,000 net improvements in human people annually. Freshwater is imperative for a few parts of day-to-day presence. Most of the water supply is utilized by the agribusiness zone, in any case, water is misplaced due to ill-advised water framework, defilement, and insufficient organization. Farmers and major agrarian workplaces should set water capability standards to cut squandering. Around 70% of the water utilized by and large comes from farms; of that 70%, a fair 30% is utilized and the overabundance 40% is wasted. Utilizing IoT and blockchain development to advance create water framework strategies and advancement was found to be a basic technique for directing water deficiency differentiated with routine ways.

Amid the arranged interaction, the going with parts speaking to things to come wastewater the official's applications were thought of:

(i) Joining with current cultivation hones and innovation.
(ii) Progressing further checking, sensors, and long battery term for a developed gadget.
(iii) The gadget should be simple to utilize, with few buttons.

9.2.1 Physical and Economic Water Wastage in Agriculture

The lack of utilization and the board of water resources in cultivating techniques are insinuated as real water waste. A pointless water framework of yields causes supplement depletion and flooding. Out-of-date or inadequate water framework techniques, comparable to surge water framework, can cause flood and vanishing and result in water hardship. Vanishing and spillage from channels, water framework trenches, and other systems. Water-serious yields are being set up in dried locales without considering water availability. Water waste is furthermore inside and out and is affected by natural alteration. The money-related disappointments associated with water utilization in cultivating are recalled for monetary water misuse. Allotments that boost farmers to utilize pointless measures of water, bringing around an inefficient utilization of resources. Deficiently, cultivating creation costs routinely avoid the normal and social costs of water waste, like spring weariness, deterioration of water quality, and impacts on downstream customers. To address these issues, Internet of Things contraption has checked out temperature, plant diseases, moisture, and climate. This contraption licenses soil clamminess prerequisites for harvests to be taken after. Farmers can utilize these gadgets to take note of plants in the field and ensure perfect plant growth. Blockchain development is utilized to store this information (Fig. 9.1).

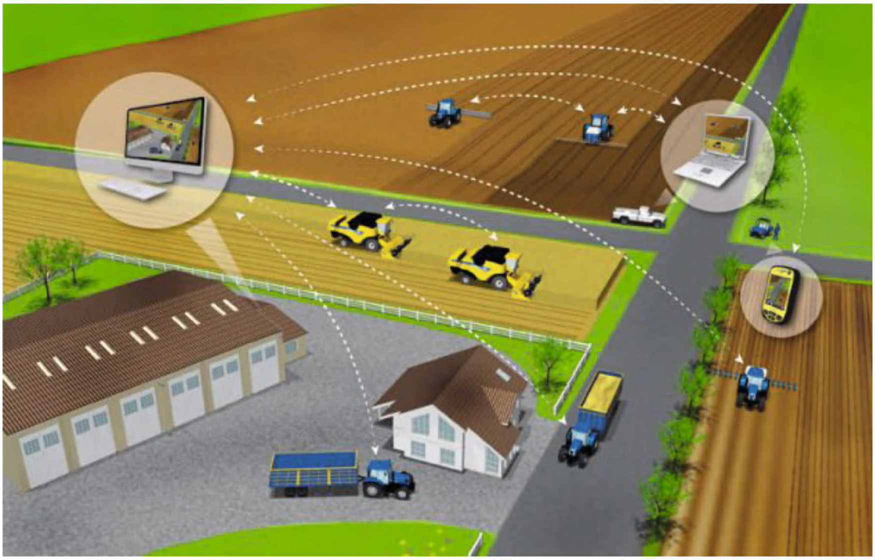


Fig. 9.1 Soil info system to the connected farm

9.2.2 Water-Saving Techniques and Tools

India's prehistoric irrigation techniques were incredibly sophisticated and complex, mostly due to their comprehension of the region's topography and climate. These techniques involved using tanks, lakes, canals, wells, and man-made reservoirs. In ancient India, the monsoon was the main determinant of irrigation. Indians in antiquity devised several techniques for gathering, storing, and distributing water for farming. A tremendous cluster of methods and innovations are utilized in cutting-edge agribusiness to be productive for nourishment, fiber, and other rural products. Advanced farming moreover utilizes various agribusiness procedures and advances that empower minimizing the utilization of fertilizers, pesticides, water, and other common assets. These developments incorporate soil observing, diverse water system frameworks, fertilizers, pesticides, edit turn, hereditary building, and exactness cultivating hones and apparatuses, like sensors. A vast array of techniques and technology are used in modern agriculture to be efficient for food, fiber, and other agricultural goods. However modern agriculture also utilizes numerous agribusiness techniques and technologies that enable minimizing the use of fertilizers, pesticides, water, and other natural resources. These innovations include soil monitoring, different irrigation systems, fertilizers, pesticides, crop rotation, genetic engineering, and precision farming practices and tools, like sensors. In recent years, this monitoring has been done by sensors. The concept of sustainable agriculture has gained traction, focusing on biodiversity, wastewater reduction, and multiple environmental and agricultural problems, including soil nutrients, wastewater management, and food security concerns. However, agriculture is also a complicated issue that concerns many economics and involves many people in the production chain.

9.2.3 Crop and Field Observation

Fields are outfitted with Internet of Things (IoT) sensors to collect data in real time, including soil moisture monitors, weather stations, and crop health sensors. Soil moisture content, temperature, humidity, rainfall, and markers of crop health are all included in this data. In order to monitor crop health and field conditions, high-resolution images are obtained through the use of drones and satellites in remote sensing.

Blockchain technology is used to analyze the gathered data in order to forecast irrigation requirements and identify abnormalities. To project future circumstances and irrigation needs, predictive modeling is used. Blockchain technology maintains transparent records of agricultural conditions, irrigation techniques, and sensor data, guaranteeing data immutability and accuracy. With the use of this integrated method, automated irrigation systems may optimize water usage and increase crop yields by adjusting water delivery based on real-time data. Advisory services provide farmers with practical suggestions to help them make well-informed decisions. All

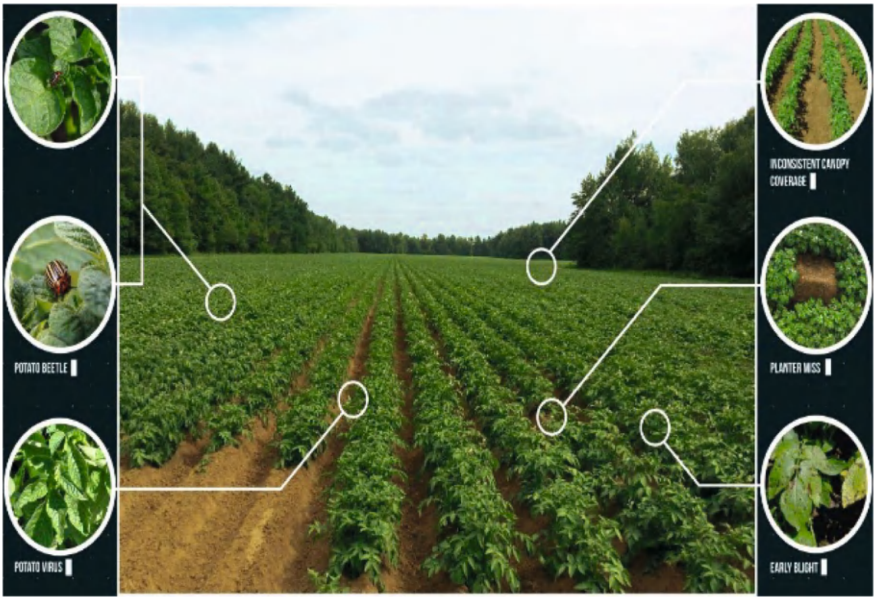


Fig. 9.2 Crop and field observation

things considered, this approach encourages water efficiency, raises crop yields and health, and strengthens climate resilience by adjusting to shifting environmental circumstances (Fig. 9.2).

9.2.4 Water Footprint (WF) Assessment Strategies

With an evaluated 1047 billion cubic meters per year (BCM/year) of WF, India leads the world in adding up to WF, taken after by China and the USA. To guarantee feasible edit yield in India, WF must be appropriately overseen. Understanding the coordinate and backhanded employments of water in different exercises is made less demanding with the utilization of the water impression evaluation. WF modeling makes a difference in recognizing the inadequacies and impacts of the current edit generation framework in trim production. Water efficiency can be upgraded and maintainable water utilization can be energized by distinguishing zones of defenselessness appraisal all through time and over distinctive geographies. IoT sensors can track water utilization at distinctive stages of mechanical or agrarian forms. Water quality, water system levels, volume devoured, and water stream rates are a few of the parameters that these sensors can evaluate. The sensors wirelessly send the water utilization information they are persistently gathering to a centralized information administration framework. Precise checking of water utilization designs and the distinguishing proof of locales appropriate for preservation measures can be made conceivable by this real-time information collection. It is conceivable to compute water impression appraisals utilizing the sensor information. The add up to the sum of freshwater devoured, both straightforwardly and in a roundabout way, in the generation of products and administrations is measured as the "water impression." The water impression for a given item, preparation, or movement can be discovered by looking at information on water utilization from different supply chains or stages of production. A blockchain record can be utilized to safely record the water utilization information and the water impression assessments that have been computed. Sometime recently any information section is included in the decentralized and unchangeable blockchain organizes, it is scrambled and timestamped. By doing this, the water impression information is ensured to be straightforward and free from control or obstructions. Keen contracts are used to consequently comply with maintainability measures or water utilization limits.

9.2.5 Storing of Information Using IoT and Blockchain Technology

IoT sensors are used to detect and store a variety of data, including nutrient levels, temperature, humidity, light intensity, field observations, plant growth, wastewater management, and plant disease prediction. Precision farming uses IoT-based technologies to monitor a wide range of agricultural variables. IoT provides vital real-time data on crop, soil, water, and air conditions for enhanced environmental protection and sustainable agriculture output. As opposed to an equipment that measures, identifies, and converts physical or chemical quantities into signals is called a sensor. Field observation, plant disease detection, crop growth tracking, temperature and humidity monitoring, soil quality monitoring, and soil type identification are all made possible by the use of IoT sensors. These information are put away in an app utilizing blockchain technology. Blockchain technology provides secure storage of information.

9.3 System Architecture

See Fig. 9.3.

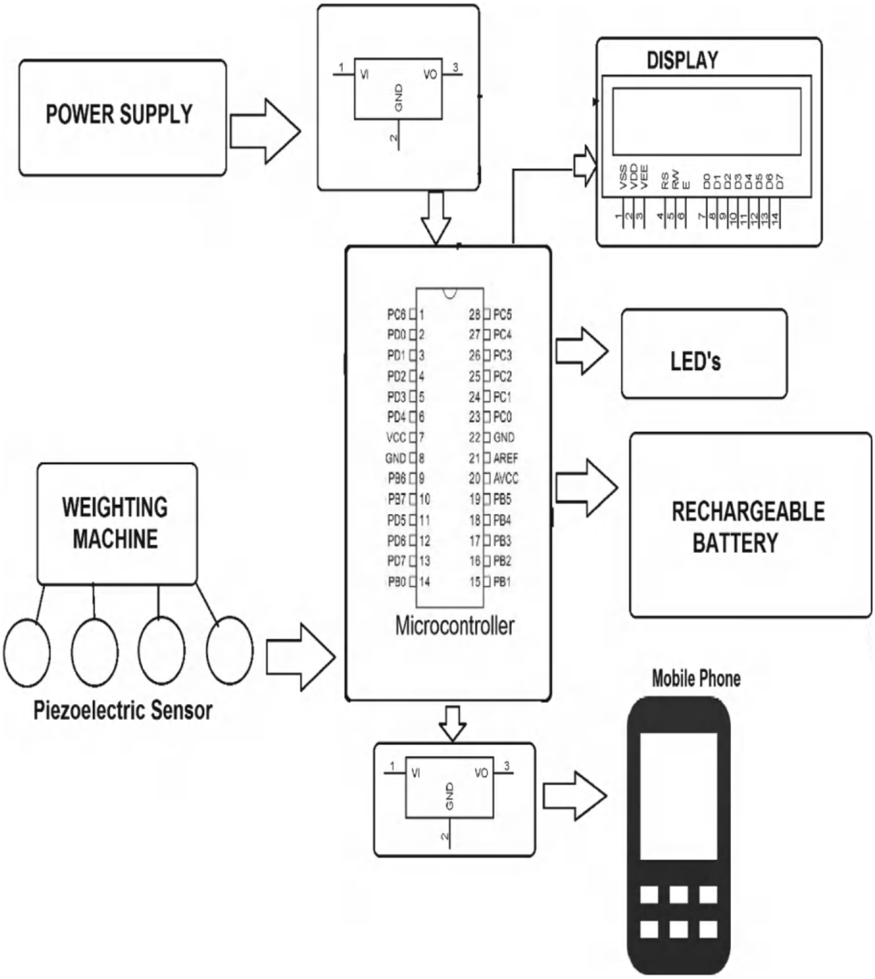


Fig. 9.3 System architecture

9.3.1 Components

- Arduino mega,
- Wi-Fi module,
- Temperature sensor,
- Soil moisture sensor,
- Light sensor,
- Pump and DC fan,
- Relays,
- Resistors,

- Capacitors,
- Transistors,
- Cables and connectors,
- Diodes,
- PCB and breadboards,
- LED,
- Transformer/adapter,
- Push buttons,
- Switch,
- IC, and
- IC sockets.
- **Arduino Mega**

Water management and intelligent irrigation systems employ Arduino Mega. The model has been selected because of its broad community support, ease of use, and versatility. In more complicated systems with several sensor inputs and outputs, the Arduino Mega is the ideal board. Additionally, projects requiring integrated Wi-Fi or other communication capabilities can use the Arduino MKR series, including the Arduino MKR Wi-Fi 1010 (Fig. 9.4).

b. **Wi-Fi Module**

A Wi-Fi module is a fully integrated wireless communication product. It contains a Wi-Fi chip and an application host processor, enabling Wi-Fi transmission and

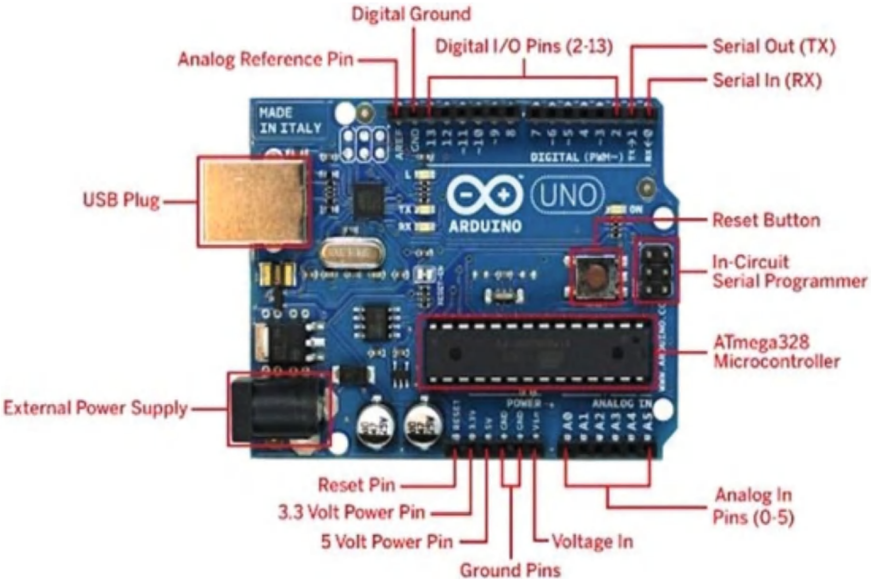


Fig. 9.4 Arduino mega

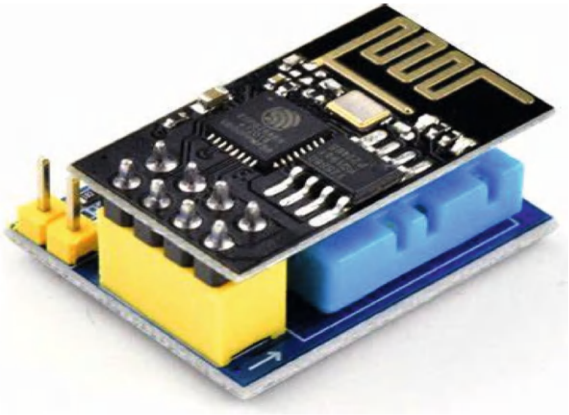


Fig. 9.5 Wi-Fi module

reception. It can plug into a network and broadcast Wi-Fi signals to smart devices such as laptops and phones. It is used for the development of end-point IoT (Internet of Things) applications. Some examples of Wi-Fi modules are Espressif Systems (ESP8266) (Fig. 9.5).

c. **Sensors**

A sensor may be a gadget that recognizes or measures a particular physical property and produces a yield flag in response. A sensor is an input gadget that gives a yield (flag) related to a particular physical amount. It changes over signals from one vitality space into an electrical space. Arduino boards are used to connect various sensors that measure soil moisture, temperature, humidity, and other environmental parameters essential for effective irrigation management.

d. **Soil Sensor**

Soil sensors are disobedient utilized to screen soil conditions. They can track different characteristics such as dampness, conductivity, temperature, supplements, pH, and saltiness. These sensors give real-time information collection and investigation, making a difference in progress trim administration and general generation (Fig. 9.6).

e. **Temperature Sensor**

A soil temperature sensor could be a gadget utilized to degree and screen the temperature of the soil. It makes a difference to decide the ideal time for planting or sowing in your cultivate. These sensors come in different plans, counting thermistors, thermocouples, thermocouple wires, and averaging thermocouples. They give important information for scientific-grade surface vitality adjust estimations (Fig. 9.7).

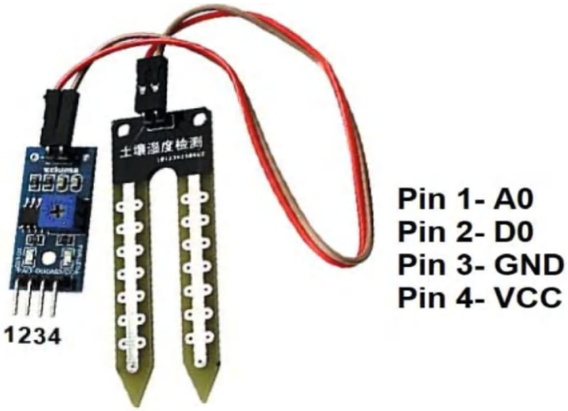


Fig. 9.6 Soil sensor

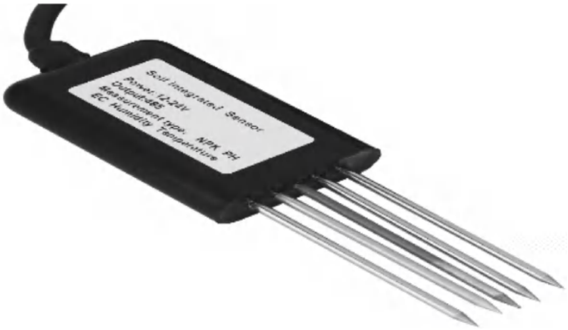


Fig. 9.7 Temperature sensor

f. **Pump and DC Fan**

A pump is utilized to provide water to the soil when it gets too dry. The framework intermittently peruses the soil dampness level employing a capacitive soil dampness sensor. If the dampness level falls below a certain limit (demonstrating dry soil), the Arduino actuates a hand-off, which turns on the pump. The pump at that point conveys water to the soil, guaranteeing legitimate hydration for plants. Alternately, in case the soil is enough sodden, the transfer deactivates the pump. This mechanized handle makes a difference keeping up ideal soil dampness levels for plant growth. Some frameworks moreover join a DC fan to upgrade and discuss circulation around the soil. The fan makes a difference in anticipating over-the-top dampness buildup, particularly in encased environments. Proper discussion circulation avoids form development and guarantees uniform soil dampness dissemination (Fig. 9.8).

g. **Relays**

Soil dampness sensors utilize diodes to degree the electrical resistance of the soil. Particularly, they utilize two metal tests that evaluate how troublesome it is for power to stream through the soil. This resistance estimation gives data on soil dampness

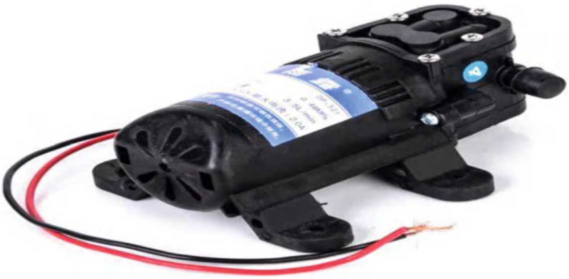


Fig. 9.8 Pump

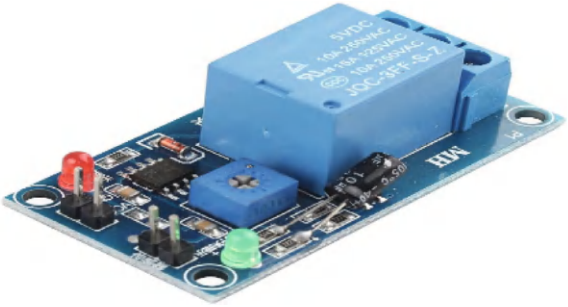


Fig. 9.9 Relay

levels. The diodes play a significant part in this handle, permitting the sensor to gauge dampness viably (Fig. 9.9).

h. **Resistors**

Soil dampness sensors utilize electrical resistance to degree the dampness substance in soil. These sensors regularly comprise of two cathodes implanted within the soil. As the soil gets to be more immersed with water, its electrical conductivity increments, coming about in a lower resistance esteem. Be beyond any doubt that moisture alone is not sufficient to realize low resistivity; the soil must moreover contain mineral salts to make an electrolyte that conducts power.

i. **Capacitance**

Capacitance sensors utilize two tests (one with a positive charge and one with a negative charge) to make an electromagnetic field as said above. This permits them to degree the charge-storing capacity of the fabric between the tests (the soil) which can at that point be related to the sum of water within the soil that's being measured (Fig. 9.10).

j. **Transistors**

Transistors in soil dampness are utilized in electronic sensors to degree and screen the water substance in the soil. These sensors ordinarily utilize the properties of transistors to distinguish changes in soil resistance or capacitance, which relate to the

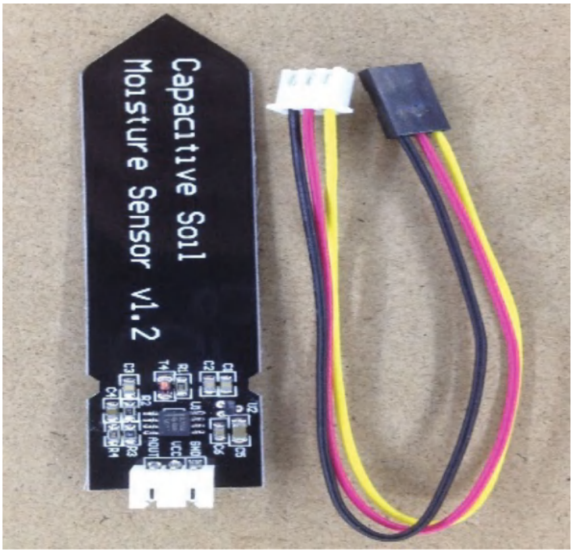


Fig. 9.10 Capacitance

soil's dampness levels. The transistors act as switches or enhancers within the sensor circuits, empowering the transformation of analog signals into computerized information that can be processed and deciphered to supply precise dampness readings. This innovation is vital for rural applications, water system frameworks, and natural checking, making a difference in optimizing water utilization and moving forward trim abdicate (Fig. 9.11).

k. **Diodes**

Soil dampness sensors utilize diodes to degree the electrical resistance of the soil. Particularly, they utilize two metal tests that evaluate how troublesome it is for power to stream through the soil. This resistance estimation gives data on soil dampness

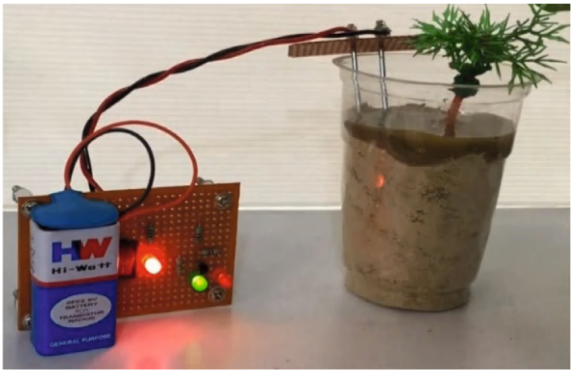


Fig. 9.11 Transistors

Fig. 9.12 Diodes

levels. The diodes play a pivotal part in this handle, permitting the sensor to gauge dampness viably (Fig. 9.12).

l. **PCB and Breadboards**

PCBs are utilized to make a compact, solid, and organized circuit for the soil dampness sensor system. PCBs have components just like the soil dampness sensor, microcontroller, and transfer driver IC. These components are associated through follows on the PCB. The PCB encourages flag preparation by interfacing the sensor with an op-amp comparator and the microcontroller. The hand-off on the PCB controls the water pump engine based on soil dampness information. Breadboards are transitory prototyping stages for testing and amassing electronic circuits. Breadboards permit fast experimentation without patching. Components can be stopped and modified easily. Before planning a changeless PCB, engineers utilize breadboards to approve the circuit plan (Fig. 9.13).

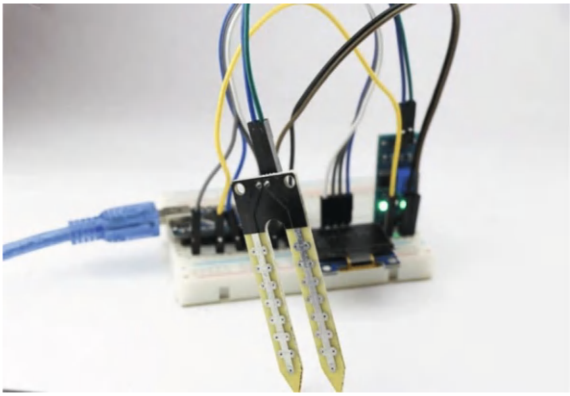


Fig. 9.13 Breadboards

Fig. 9.14 IC socket

m. **IC Sockets**

A soil dampness sensor may be a low-cost electronic gadget utilized to distinguish the dampness substance in the soil. It regularly comprises two primary parts: the soil dampness test and the soil dampness module. When embedded into the soil, the metal plates come into contact with the soil dampness, and the sensor measures the electrical resistance between the two anodes. The more dampness displayed within the soil, the lower the electrical resistance between the cathodes (Fig. 9.14).

9.4 Parameter Measured

a. **Temperature**

One of the crucial irrigation parameters is temperature. Temperature sensors are used to gauge ambient temperature and record daily data utilizing blockchain technology. Sensors are used to measure two different temperatures: the temperature of the soil and the temperature of the atmosphere (Fig. 9.15).

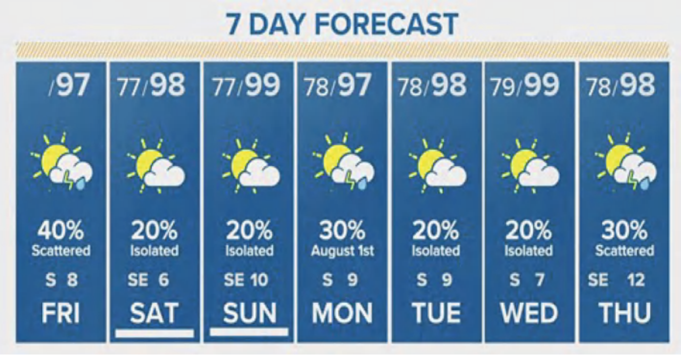
b. **Weather Forecasting**

In farming, weather forecasting is the process of estimating a location's atmospheric conditions at a specific moment to determine whether or not it is suitable for agricultural operations. With the use of sensors and geographic and meteorological data, farmers can utilize agricultural weather prediction technologies to get their fields ready for unusual or severe weather. Agribusinesses use weather forecasting devices to track changes in the global environment and anticipate natural calamities like floods and temperature spikes (Fig. 9.16).

c. **Humidity**

The ratio of air's vapor pressure to its saturation vapor pressure is known as the humidity of the air. A food product's equilibrium relative humidity (ERH) is the air

Fig. 9.15 Temperature



7 DAY FORECAST

FRI	SAT	SUN	MON	TUE	WED	THU
/97	77/98	77/99	78/97	78/98	79/99	78/98
40% Scattered	20% Isolated	20% Isolated	30% August 1st	20% Isolated	20% Isolated	30% Scattered
S 8	SE 6	SE 10	S 9	S 9	S 7	SE 12

Fig. 9.16 Weather forecasting

surrounding it at a relative humidity that balances with its surroundings. Relative humidity (RH), which is the ratio of the amount of water vapor in the air to the maximum amount the air can hold at a given temperature, is used to measure it.

d. Light Intensity

The entire amount of light that plants get is referred to as light quantity or light intensity. It can also mean the amount of brightness to which a plant is exposed. The description of light intensity disregards wavelength and color, in contrast to light quality. It specifies the quantity of light photons in the photosynthetic waveband that a square meter of space gets in a second. It is quantifiable with a light meter.

e. Soil Moisture

The water content of the soil is known as soil moisture. It can be described in weight or volume units. The most important factor in agriculture is soil moisture. Plants may

Fig. 9.17 Soil moisture

perish from a lack of water or an excess of it. This data is dependent on numerous external elements at the same time, chief among them being variations in the weather and climate. This is why knowing the best techniques for determining the moisture content of soil is so important (Fig. 9.17).

f. Detection of Nutrient Levels in Soil

The soil test is a quick method for determining the soil's macronutrient content. It contains colorimetry, which measures the three primary macronutrients (nitrogen, phosphorus, and potassium) subjectively, as well as the dirt's pH level, which lays out the dirt's sharpness, impartiality, or basicity. Farmers can monitor the nutrients in their soil using the sensor to help their plants grow to their full potential. The sensor measures the electrical conductivity of the soil, which is directly related to the amount of nutrients present (Fig. 9.18).

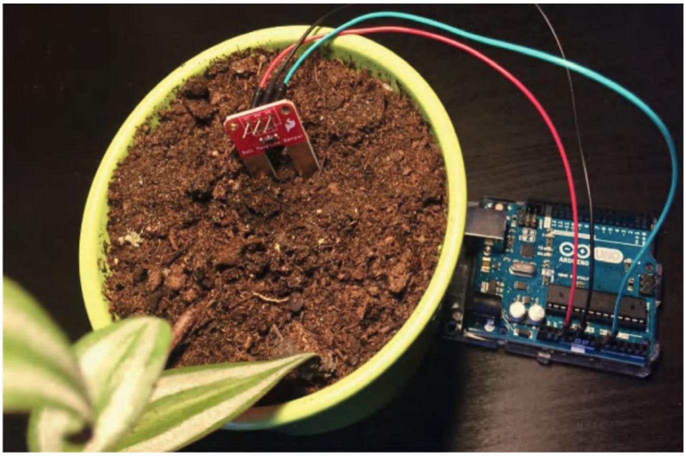


Fig. 9.18 Detection of nutrient levels in the soil

Fig. 9.19 Plant disease prediction

g. Plant Disease Prediction

Plant diseases negatively impact agricultural productivity. Plant diseases must be rapidly recognized to prevent an increase in food poverty. Because effective prevention and treatment of plant diseases depend on early diagnosis, plant diseases are a significant management and decision-making issue in agriculture. Diseased plants usually have obvious lesions or marks on their stems, leaves, flowers, or fruits. Every disease or pest issue typically has a unique external pattern that can be used to recognize abnormalities in a particular way. Plant diseases are detected using a variety of sensors. Additionally, blockchain technology is used to store these data. Farmers will be able to salvage their plants if plant diseases are discovered early (Fig. 9.19).

h. Crop Growth Tracking

Each plant has an ideal soil pH condition, and most plants battle to develop appropriately when the pH is either as well tall or as well moo. Employing a soil pH sensor to degree soil sharpness or alkalinity is useful for trim development and makes a difference in decreasing the event of bugs and infections. Subsequently, soil pH testing is basic for rural purposes. Nitrogen is the essential constituent of proteins and plays a significant part in advancing stem and leaf development as well as natural product advancement. Phosphorus encourages blossom bud separation and early blooming and fruiting in tomatoes. Potassium is mindful for advancing tough stems and upgrading plant resistance to cold, whereas moreover expanding sugar substance and vitamin C levels in natural products. Soil NPK sensors can identify nitrogen, phosphorus, potassium, and other elements within the soil to supply the supplements required by plants and advance plant development. Adjusting the level of water is additionally vital for edit development. The following is done utilizing sensors. All the information is put away utilizing blockchain innovation.

i. Soil Quality Monitoring

Rebellious for evaluating soil quality incorporate soil sensors. They can be partitioned into sensors that keep an eye on saltiness, pH, temperature, conductivity, supplements, and dampness. Soil sensors are the collective term for all these numerous sorts of gadgets. More modern soil sensors are presently accessible much obliged to innovative improvements, and they can screen temperature, conductivity, supplement substance, and soil dampness all at once. Soil sensors are frequently composed of a detecting component that measures different parameters of the soil, such as temperature, dampness substance, pH esteem, and electrical conductivity. The sensor component changes over the measured information into electrical driving forces. The inner circuitry of the sensor regularly changes over these signals into advanced arranges for simpler preparation and transmission. Advanced signals are transmitted wirelessly or associated with a computer or controller. In arrangement to extricate valuable information, such as the pH, temperature, and soil dampness substance, the computer or controller gets the computerized signals, forms, and analyzes the data. The controller's capability to consequently control related gadgets, such as water system frameworks and climate stations, depending on the analysis's discoveries, makes mechanized administration attainable (Fig. 9.20).

j. Soil Type Identification

The upper layer of soil in which plants develop is known as soil. There are diverse sorts of soils like ruddy soil, brown soil, dark soil, loamy soil, sandy clay, and silty clay. These sorts of soil are recognized utilizing sensors and identify the water level according to the soil sort, dampness, and temperature. Sensors will change over these data as computerized data and put away utilizing blockchain innovation.

Fig. 9.20 Soil quality monitoring

k. **Water Management**

Water administration in horticulture is vital for economical trim generation and asset preservation. One viable approach is an accurate water system, which leverages innovation to optimize water utilization based on trim needs and natural factors. The rancher can utilize this data to coordinate more dampness to the dryer ranges where it is most required, maintaining a strategic distance from waterlogging and squandering assets in wetter ranges. This way, rural water administration based on soil dampness levels will progress asset assignment, avoid plant push, and increment agrarian yields. Soil dampness sensors are priceless instruments for accuracy agribusiness, making a difference for agriculturalists to guarantee ideal water levels in their soil. Utilizing these sensors, they can precisely degree the dampness within the soil, making it simpler to decide when the water system is fundamental and decrease the wastage of valuable assets. All this information is put away utilizing blockchain innovation. This makes a difference for the agriculturists to check the water level, trim quality, and other parameters through portable.

9.5 Telegram Message

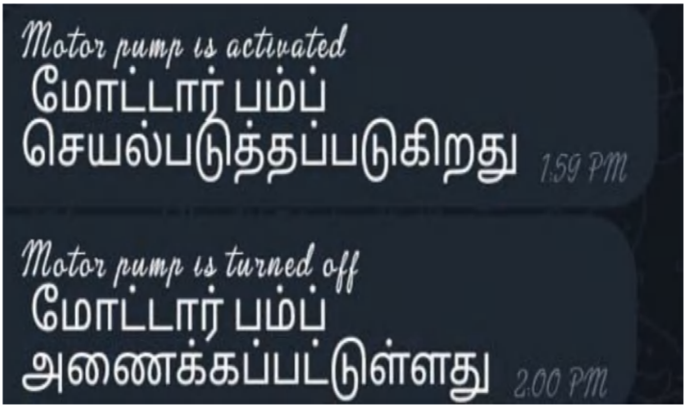
Agriculture may be an imperative industry that requires opportune communication, productive operations, and proactive administration. Wire notices and alarms have developed as solid and proficient arrangements for upgrading communication and streamlining rural hones. By leveraging the control of content information, agriculturists, agrarian businesses, and partners can remain educated about basic data, get convenient overhauls, and improve overall efficiency. This wire message is worn out a rancher convenient dialect. Wire notices and cautions can advantage the horticulture division from climate advisories and showcase overhauls to hardware support updates and bug administration notices. By receiving wire notices, the farming industry can optimize operations, make educated choices, and maximize surrender (Fig. 9.21).

9.6 Internet of Things in Agriculture

IoT technology uses sensors and networked devices to gather and process data in real time. IoT sensors in agriculture may track temperature, humidity, soil moisture content, and other vital metrics, giving accurate data for effective water management.

(1) **Blockchain in the Field of Agriculture**

A decentralized and transparent way to record transactions and data is provided by blockchain technology. Blockchain technology can improve data security, guarantee traceability, and offer a trustworthy platform for information sharing among stakeholders in the agricultural industry.



Motor pump is activated
மோட்டார் பம்ப் செயல்படுத்தப்படுகிறது 1:59 PM

Motor pump is turned off
மோட்டார் பம்ப் அணைக்கப்பட்டுள்ளது 2:00 PM

Fig. 9.21 Telegram message

(2) **Blockchain Connectivity**

To guarantee data integrity, transparency, and security, blockchain systems can be loaded with the data that Arduino has acquired. This is essential for monitoring and validating irrigation techniques and guaranteeing water use that is sustainable.

(3) **Smart Contracts**

On the blockchain, automated contracts, also known as smart contracts, can be configured to do particular tasks in response to predetermined criteria. A smart contract might, for instance, pay suppliers automatically when specific irrigation benchmarks are reached.

(4) **Intelligent Watering Systems**

IoT sensors are utilized by smart irrigation systems to gather information on soil and ambient conditions, which is then used to optimize water utilization. By supplying the appropriate amount of water at the appropriate time, these systems can drastically minimize water wastage and increase crop yields.

9.7 Methodology

a. **System Architecture**

The suggested smart irrigation system consists of a central control unit, blockchain technology, and Internet of Things sensors. The central control unit receives data from the Internet of Things sensors, which track temperature, moisture content in the soil, and other pertinent variables. All data transactions are recorded by the blockchain network, guaranteeing security and transparency.

b. **Data Collection and Analysis**

The best irrigation schedule is determined by analyzing data gathered from IoT devices. Utilizing past data and meteorological predictions, machine learning algorithms can be used to forecast water requirements. Every decision and piece of information is recorded on the blockchain, creating an auditable and unchangeable ledger.

9.8 Outcomes

a. **Water Sustainability**

Water efficiency has significantly improved with smart irrigation systems. As adjusting irrigation schedules based on real-time data, water consumption can be lowered by up to 30% as compared to conventional watering techniques.

b. **Harvest Productivity**

Crop yields have grown as a result of optimized irrigation schedules. Our case studies show that smart irrigation systems can increase food security by improving crop yields by an average of 20%.

c. **Resilience to Climate Change**

One important advantage of smart irrigation systems is their capacity to adjust to shifting weather patterns. These technologies lessen the effects of climate change on agriculture by continuously monitoring the surrounding environment and modifying irrigation techniques.

9.9 Conclusion

Successful wastewater administration in farming is basic for advancing maintainable cultivating hones, securing water assets, and guaranteeing natural well-being. Executing coordinated administration techniques that combine progressed treatment advances, productive water system hones, and administrative systems will lead to more flexible agrarian frameworks. Emphasizing instruction and collaboration among partners is significant for cultivating development and selection of best hones. Eventually, a comprehensive approach to wastewater administration in farming not only bolsters nourishment security but also contributes to the by and large well-being of environments and communities. This framework is valuable for way better farming practices and water can be spared in horticulture. This strategy is precious for trim development and water sparing. All this data is put away in an app utilizing blockchain innovation. Water administration and parameters measured can be seen and accessed through mobile. It can improve soil quality, edit quality, and anticipate plant illnesses. It additionally decreases water wastage in agriculture.

References

Bodkhe U, Tanwar S, Bhattacharya P, Kumar N (2020) Blockchain for precision irrigation: opportunities and challenges. Emerg Telecommun Technol

Dey K, Shekhawat U (2021) Blockchain for sustainable e-agriculture: literature review, architecture for data management, and implications. ScienceDirect

Drăgulinescu A-M, Constantin F, Orza O, Bosoc S, Streche R, Negoita A, Osiac F, Balaceanu C, Suciu G (2021) Smart watering system security technologies using blockchain. IEEE

Harvey CA, Chacón M, Donatti CI, Garen E, Hannah L, Andrade A, Bede L, Brown D, Calle A, Chará J, Clement C, Gray E, Hoang MH, Minang P, Rodríguez AM, Seeberg-Elverfeldt C, Semroc B, Shames S, Smukler S, Somarriba E, Torquebiau E, van Etten J, Wollenberg E (2014) Climate-smart landscapes: opportunities and challenges for integrating adaptation and mitigation in tropical agriculture. Conserv Lett 7

Jararweh Y, Fatima S, Jarrah M, AlZu'bi S (2023) Smart and sustainable agriculture: fundamentals, enabling technologies, and future directions. ScienceDirect 110

Javaid M, Haleem A, Singh RP, Suman R (2022) Enhancing smart farming through the applications of agriculture 4.0 technologies. Int J Intell Netw. ScienceDirect 3

Jiang P, Zhang L, You S, Fan YV, Tan RR, Klemeš JJ, You F (2023) Blockchain technology applications in waste management: overview, challenges and opportunities. J Clean Prod Sciencedirect 421

Karunathilake EMBM, Le AT, Heo S, Chung YS, Mansoor S (2023) The path to smart farming: innovations and opportunities in precision agriculture. MDPI

Krithika LB (2022) Survey on the applications of blockchain in agriculture. MDPI

Kouhizadeh M, Saberi S, Sarkis J (2020) Blockchain technology and the sustainable supply chain: theoretically exploring adoption barriers. Int J Prod Econ ScienceDirect 231

Lin W, Huang X, Fang H, Wang V, Hua Y, Wang J, Yin H, Yi D, Yau L (2018) Blockchain technology in current agricultural systems: From techniques to applications. IEEE

Liu W, Shao X-F, Wu C-H, Qiao P (2021) A systematic literature review on applications of information and communication technologies and blockchain technologies for precision agriculture development. J Clean Prod. ScienceDirect 298

Ma X, Yuan H, Du W (2024) Blockchain-enabled construction and demolition waste management: advancing information management for enhanced sustainability and efficiency. MDPI

Marzougui F, Elleuch M, Kherallah M (2024) IoT and blockchain in agriculture: architecture and research issues. Springer

Quy VK, Hau NV, Anh DV, Quy NM, Ban NT, Lanza S, Randazzo G, Muzirafuti A (2022) IoT-enabled smart agriculture: architecture, applications, and challenges. MDPI

Rabadiya Kinjal A, Shivangi Patel B, Chintan Bhatt C (2017) Smart irrigation: towards next generation agriculture. Springer, pp 265–282

Ragab MA, Badreldeen MM, Sedhom A, Mamdouh WM (2022) IoT-based smart irrigation. Int J Ind Sustain Dev 3

Sarfraz S, Ali F, Hameed A, Ahmad Z, Riaz K (2023) Sustainable agriculture through technological innovations. Springer, pp 223–239

Sharma P, Shukla S, Vasudeva A (2021) Trust-based opportunistic network offloaders for smart agriculture. Int J Agric Environ Inf Syst (IJAEIS)

Sivakumar E, Ganesan G, Ragavi (2022) Harnessing I4.0 technologies for climate smart agriculture and food security. ACM J

Tian F (2016) An agri-food supply chain traceability system for China based on RFID & blockchain technology. IEEE

Tripoli M, Schmidhuber J (2018) Emerging opportunities for the application of blockchain in the agri-food industry. Food Agriculture Organization of the United Nations (FAO)

Ur Rehman K, Andleeb S, Ashfaq M, Akram N, Akram MW (2023) Blockchain-enabled smart agriculture: Enhancing data-driven decision making and ensuring food security. J Clean Prod 427. ScienceDirect

Verdouw CN, Wolfert J, Beulens AJM, Rialland A (2016) Virtualization of food supply chains with the internet of things. J Food Eng ScienceDirect 176

Waluyo, Widura A, Hadiatna F, Anugerah D (2023) Fuzzy-based smart farming and consumed energy comparison using the internet of things. IEEE

Wanyama J, Bwambale E, Kiraga S, Katimbo A, Nakawuka P, Kabenge I, Oluk I (2024) A systematic review of fourth industrial revolution technologies in smart irrigation: constraints, opportunities, and future prospects for sub-Saharan Africa. J Clean Prod, ScienceDirect 316

Chapter 10
Blockchain Application in Sustainable Smart Water and Wastewater Management

Samra Afzal and Syed Imtiyaz Hassan

Abstract There has never been an urgent need for innovative water management solutions, as over 2 billion individuals worldwide lack reliable access to pure drinking water and 80% of wastewater is discharged untreated. This chapter explores the possible prospects of combining blockchain technology, the Internet of Things (IoT), and machine learning (ML) in urban water systems. The decentralized and secure ledger architecture of blockchain offers superior transparency and data integrity, which are essential in making resource allocation and monitoring truly effective. Where IoT devices deliver accurate information about the quality and movement of water in real time and where machine learning algorithms can help with optimized water distribution and predictive maintenance, water management systems are becoming smarter and more adaptable. This chapter reviews the challenges of today and provides technical analysis alongside real-world examples of how each can enable us to address water scarcity, pollution, and inefficient distribution. Through a thorough examination of current topics and practical examples, the chapter discusses how blockchain technology could tackle issues such as water scarcity, pollution, and inefficient distribution. Case examples, such as the almost disastrous drought in Cape Town and the water crisis in Flint, highlight the urgent requirement for robust infrastructure and effective governance. These results have considerable impacts on the economy, environment, and social development, supporting the transition of smart cities to more advanced and sustainable water management practices. This chapter is expected to contribute to continuously improving and detailed research and studies, create a pathway for implementing sustainable urban water and wastewater systems and secure those systems to be able to face the future challenges of increasing urban population and climate change.

Keywords Blockchain technology · IoT · Machine learning · Smart water · Wastewater management · Sustainable · Smart city

S. Afzal · S. I. Hassan (✉)
Department of Computer Science and Information Technology, School of Technology, Maulana Azad National Urdu University (Central University), Hyderabad, India
e-mail: s.imtiyaz@gmail.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2025

K. Ahmad et al. (eds.), *Fostering Machine Learning and IoT for Blockchain Technology*,
Transactions on Computer Systems and Networks,
https://doi.org/10.1007/978-981-96-4074-4_10

10.1 Introduction

According to the United Nations in 2021, there are over 2 billion people without reliable access to clean drinking water and about 80% of wastewater in the world is discharged without being treated leading to enormous health risks as well as environmental degradation (United Nations 2018, 2022). The need to manage water scarcity and pollution cannot be overstated, especially as urban populations expand. It is expected that the population in cities will increase to 66%, from 55% of people living in urban areas in 2018, by 2050 (United Nations 2023). Since water resources are already limited, the rapid growth of urbanization demands innovative approaches for sustainable water supply and wastewater management.

The story of Cape Town's "Day Zero" crises in 2018 is an obvious example of the results of unfit water management. As seen in Cape Town, it was far too close to running out of water. This highlights how vulnerable urban water infrastructure can be to climate change, population growth, and maladministration of resources. Such circumstances demand for efficient, robust, and sustainable water management systems. Technologies such as blockchain technology, Internet of Things (IoT), and machine learning (ML) can effectively help address these challenges and enhance adaptability and sustainability of urban waterscapes.

Another distressing example is the Flint water issue which started in 2014. This resulted in the lead contamination in the new water supply with thousands of residents being badly affected and showed how poor management and collapsing water infrastructure can have harmful consequences (Campbell et al. 2016). Such disasters not only reflected the human suffering but also the long-term economic and social consequences of poor water management.

The UN Secretary-General António Guterres warned us, saying, *"But water is in deep trouble"*. He added, *"We are draining humanity's lifeblood through vampiric overconsumption and unsustainable use, and evaporating it through global heating. We've broken the water cycle, destroyed ecosystems and contaminated groundwater"* (United Nations 2023). This quotation encapsulates the importance of sustainable water management in our globally connected world.

Smart cities are the future of urban living, where modern technology is used to improve quality of life, optimize resource use, and promote sustainability. Smart cities are built around the reliable management of such services as water and wastewater systems. Such operations are essential for public health maintenance, economic activity promotion, and environment protection. However, common approaches to water management often suffer from low efficiency due to losses resulting from leaks, incorrect billing, or lack of decision-making data. The magnitude of water loss can even reach 50% particularly in less-developed nations caused by leakage and illegal connections (World Bank 2016).

There are multiple reasons why demand for effective and sustainable water and wastewater management systems is increasing. The resultant effects of climate change on water supply and quality have been huge challenges facing the world today. Moreover, urban water demand has been rising as a result of population increase coupled with industrialization thus exerting undue pressure on the existing infrastructure for water supply. Water resource management requires accurate information, necessary interventions in time as well as sector-wide coordination. This is where modern technologies such as blockchain, IoT, and ML come into play.

Blockchain technology, first proposed by Satoshi Nakamoto in 2008 with the development of Bitcoin, has moved past its original use in cyber-currencies (Nakamoto 2008). It provides a decentralized, transparent, and secure means for transactions registry and data management. Blockchain can enhance data integrity, promote water usage transparency and distribution as well as efficient resource allocation. For instance, the blockchain technology can be employed to construct a see-through ledger of water consumption that consequently helps the monitoring and managing of water resources.

The Internet of Things (IoT) is a term that is often used to describe a network of interconnected devices that collect and exchange real-time information. IoT devices like sensors can be used to monitor both the quality and flow rate of water in water management. In addition to this, it is also helpful in detecting leakages. Swiftly identifying failures and optimizing distribution systems for water infrastructure is facilitated by this instant data collection (Zulkifli et al. 2022). For example, water wastage can be prevented in case of leaks in water pipes by the quick identification of these IoT sensors which will notify the maintenance personnel leading to swift actions that are needed.

Machine learning (ML) may be applied in data-driven prediction that uses algorithms and statistical models for water demand predictions, anomaly detection, and optimization in both the quality of water supplied to households or industries and treatment operations (Lowe et al. 2022). Machine learning can provide suggestions to make informed decisions and will help in increased efficiency of the water management system by analyzing historical data records and identifying patterns. For example, machine learning algorithms can forecast high periods of water demand and change the direction in which the flow count should be directed to ensure efficient water supply without wastage.

By combining blockchain with IoT and ML, we can enhance water/wastewater management systems—smarter, more responsive, faster, and more efficient. Figure 10.1 provides an overview of how these technologies can enhance various aspects of water management.

The objective of this chapter is to investigate how blockchain technology, IOT, and ML could potentially be combined to improve sustainable water and wastewater management in smart cities. The aim of this research is to identify contemporary challenges faced by current water and wastewater management in relation to it; reviewing real-world use cases in this space; and also exploring potential solutions through the analysis of live deployments/case studies.

In this chapter, we made a comprehensive review of how blockchain, IoT, and ML could be used in building better water systems that are effective and sustainable. We are looking at these technologies as a way to understand their capacities for reshaping urban waterscapes in the context of escalating urbanization and climate

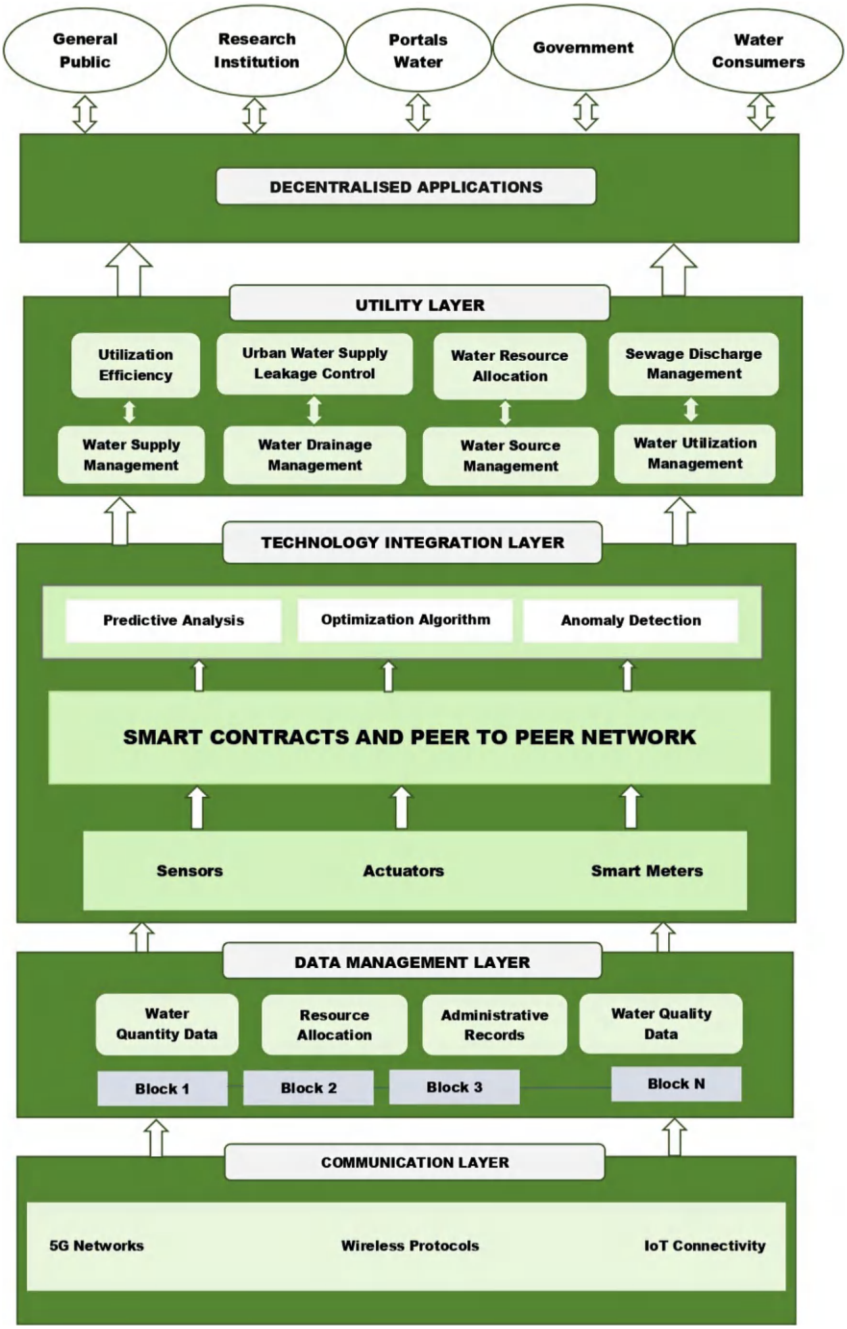


Fig. 10.1 Integration of blockchain, IoT, and machine learning in sustainable water management

change impacts. The purpose is to add to the growing literature on smart city applications while providing guidance for future research and implementation in the area of sustainable water and waste management in cities.

10.2 Smart Water Management

Imagine water with a brain able to think, predict, and communicate. That is the essence of "smart water", a game-changing way to integrate next-generation technology with one of the Earth's most precious resources. The term "smart" means connectivity to advanced technologies like the IoT, blockchain, and ML, while "water" simply refers to the life-sustaining element that these technologies aim to manage more effectively.

Smart water management (SWM) is the practice of using technology and methods to harvest, manage, and distribute this precious resource. Important themes reflected in SWM are the use of IoT devices, blockchain technology, and ML algorithms for more enhanced monitoring, analysis, and optimization pertaining to water distribution and wastewater treatment processes. More generally, such technologies will allow for real-time data collection and analysis, predictive maintenance, automated control systems, and transparent sharing of information across the wider water management ecosystem—improving overall efficiency and sustainability (The World Bank 2019).

The significance of proper water management is very high for smart cities. With the increase in population, there is a universal demand for water that leads to excessive pressure on the current water infrastructure. Water should be used judiciously which means managing water competently so as to waste it minimally, not run out of the wet stuff and keep our precious liquid product clean. Additionally, it also reduces the ecological footprint and effluent discharges in smart cities to ensure that they meet their sustainability objectives. The World Bank says that proper water management practices can result in significant economic advantages as far as reduced losses and increased productivity are concerned (United Nations 2018; The World Bank 2019).

One of the most illustrative stories about what good water management is all about happened in Cape Town in 2018. The city was on the verge of running out of water because of a severe drought and poorly managed water sources. This was crisis that revealed the need for intelligent water platforms to address a rapidly changing climate and population (United Nations 2022).

10.2.1 Current Challenges in Water Management

Even with the rapid development of technology, water management encounters multiple serious problems that prevent it from reaching the goals of sustainability. Some of the challenges include water scarcity, inefficiencies in distribution, and

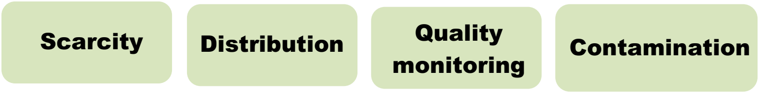


Fig. 10.2 Current challenges in water management systems

concerns around monitoring agencies' effectiveness and contamination as shown in Fig. 10.2.

10.2.1.1 Water Scarcity and Distribution Challenges

The shortage itself is, after all not so much in the lack of water but more with mismanagement. In some cities, for instance, up to half of the water put into a distribution system simply leaks out. Lost water before reaching consumers is estimated to be up to 45% in developing countries (World Bank 2016).

Outdated infrastructure and absence of real-time monitoring often result in inefficient water distribution within urban areas. Conventional water management solutions are based on manual inspections and periodic maintenance, which are not sufficient to address the dynamic nature of urban demands for water. Blockchain integrated with IoT devices can revolutionize these systems and generate up-to-date data on water flow, pressure, consumption to faster detect leaks, and unauthorized usage. Another study focused on smart water management in Barcelona found that with real-time monitoring using IoT sensors and transparent record-keeping by the help of blockchain, losses decreased around 20% parallel to providing a more reliable distribution for water supply (Naqash et al. 2023).

Blockchain technology, in particular, offers significant potential to address these challenges. Blockchain's decentralized and immutable nature ensures that data related to water distribution is secure and tamper-proof, facilitating transparent and trustworthy management practices. A study by Christidis and Devetsikiotis (2016) described that the blockchain could be one option to improve security and efficiency for IoT devices, in order to have data reliable/accurate like many people dream (Xia et al. 2022). Additionally, a framework proposed by Zheng et al. (2017) for blockchain-based water management emphasizes the role of smart contracts in automating maintenance and billing processes, further reducing operational inefficiencies (Zheng et al. 2017).

10.2.1.2 Quality Monitoring and Contamination Issues

The quality of water is monitored to maintain the safety of drinking water and effective wastewater treatment. For example, lead poisoning of over thousands of people in Flint (Campbell et al. 2016) could have been avoided. Conventional methods for monitoring water quality are typically slow and reactive, based on periodic sampling followed by laboratory analysis that can take up to a week—all of which delays identification of contamination incidents.

Smart water management is the facility that uses IoT sensors and ML algorithms to monitor various aspects of drinking water, such as pH, turbidity, or contaminant levels in real time. They are able to report irregular activities almost simultaneously, causing alarms and rapid preventive measures. Using blockchain technology, water quality data is recorded securely and shared transparently among different parties, increasing trust in the data and accountability. For example, a blockchain-based water quality monitoring system for rivers in Malaysia has been proposed that includes the use of IoT for real-time monitoring and data integrity, with the development of green smart river monitoring system ensuring water quality monitoring without pollution and blockchain technology for the secure water quality management (Tajudin et al. 2024).

In addition, ML-enabled predictive analytics can predict contamination points by analyzing waypoints from historical and pattern recognition data. This proactive approach ensures timely action, like adapting water treatment processes or alerting the public, to avoid health risks and uphold trust in the safety of available drinking water.

A study by Xia et al. (2022) proposed a comprehensive framework that combines the connection of smart water system with IoT and blockchain. It pays attention to how drinking water quality monitoring and incident responsiveness can be improved by these emerging sensing technologies. Automated, real-time data systems enable cities to improve water safety and resource management on a large scale.

Another relevent study by Kavya et al. (2023) used the ML algorithms for generating predictive model of water demand to facilitate efficient planning and resource allocation in urban areas. The integration of these technologies results in synergized impact on the overall performance and sustainability of water management systems.

To sum it up, though the water management problems are large in numbers but with the integration of advanced technologies, such as IoT, Blockchain, and ML, there certainly is a sliver lining. These could revolutionize traditional water management structures into smart, efficient, and sustainable constructs that can adapt to the ever-changing requirements of today’s modern urban landscapes.

10.3 Wastewater Management

Waste means any material which is thrown away after primary use, no longer useful, or which is defective. This includes solid waste, liquid waste, and gaseous waste, where liquid waste is made up of wastewater produced by domestic, industrial, and commercial activities. Water is a basic resource that is essential for life and is necessary in various bio-chemical and physical processes. Water gets polluted with different substances in various sectors like household, industry, or agriculture and thereby transforms into wastewater.

Wastewater is any water that has been negatively affected in quality due to anthropogenic influence. That includes items such as human waste, food scraps, oils, soaps, and chemicals. In cities, typically wastewater is disposed off into sewers, treated at wastewater treatment plants and then is allowed to flow into water bodies or reused for other purposes. The development of wastewater sewage treatment has made it necessary to effectively manage this valuable resource in order to remove contaminants to avoid environmental pollution as well as minimize public health hazard and conserve water resources.

By incorporating technology such as the IoT, machine learning, and blockchain, smart wastewater management improves wastewater treatment to be more efficient, transparent, and sustainable (Farooqi et al. 2019). IoT sensors can measure water quality parameters, such as pH, turbidity, or contaminant levels in real time (Zulkifli et al. 2022; Hakak et al. 2020), which is very useful for making timely interventions and decisions. These data are analyzed through machine learning algorithms to predict potential issues and making the treatment process optimal; utilizing blockchain technology ensures integrity and transparency in records across the management system (Xia et al. 2022).

Urban sustainability relies heavily on management of wastewater. The amount of wastewater that a city produces increases rapidly with the growth in cities and population, which places more demands on their infrastructure. Ineffective water or wastewater management can be dangerous because it will result in helath risks due to pollution and resource waste. This includes, for example, untreated or insufficiently treated wastewater ending up in drinking water sources, spread diseases, and destroy ecosystems (Radcliffe and Page 2020).

These challenges are addressed by smart systems for management of wastewater as they improve the resource efficiency and reduce the operational costs (Radcliffe and Page 2020). This can further enable the reuse of treated wastewater for various non-potable applications, such as irrigation, industrial operations, and replenishing aquifers to protect freshwater resources (Dada et al. 2024). Additionally they support compliance with legislation and environmental standards through monitoring and reporting also.

10.3.1 Current Challenges in Wastewater Management

10.3.1.1 Treatment and Recycling Challenges

One bottleneck in wastewater management is ensuring that the treated and recycled water meets the quality standards. Notably, traditional treatment facilities often face issues like aging infrastructure, high energy demand, and deficiencies in terms of removal of pollutants (Singh et al. 2023). These treatment processes can be optimized with smart technologies which use real-time data analysis and machine learning algorithms.

For example, an application of an IoT-based monitoring system includes the integration with membrane bioreactors (MBRs) to improve treatment performance and decrease energy consumption (Zhang et al. 2021). Even with these advancements, there remains the challenge to scale up the systems to handle large volumes of wastewater in highly populated areas.

10.3.1.2 Monitoring and Regulatory Compliance Issues

Ensuring that wastewater management meets requirements involves following quality and environmental guidelines established by both local and global governing bodies. Conventional monitoring systems often lack the ability to collect and analyze data in time causing delays, in identifying and addressing breaches of compliance (Bułkowska et al. 2023).

Blockchain technology offers a solution to these challenges by offering an transparent platform for recording and sharing data. It ensures that all parties involved have access to tamper-proof records of wastewater treatment processes and quality standards (Hakak et al. 2020; Bułkowska et al. 2023; Dogo et al. 2019). For example, a system based on blockchain technology can streamline compliance reporting which minimizes the risk of data tampering and fosters accountability, among operators and regulators (Dogo et al. 2019).

Singapore's Public Utilities Board (PUB) is leading the way in incorporating technologies into wastewater management. By utilizing sensors and data analysis PUB has enhanced its wastewater management system to produce quality reclaimed water for non-potable purposes. This innovative system constantly monitors factors in real time, ensuring efficient and effective treatment processes. The integration of these technologies has resulted in enhancements in water quality and operational effectiveness highlighting the advantages of wastewater management (PUB 2018). Barcelona has implemented a blockchain-powered system to improve the monitoring and openness of its wastewater management procedures. This technology securely stores all details concerning wastewater treatment guaranteeing data accuracy and availability to everyone involved. By using blockchain Barcelona has boosted its adherence to rules and streamlined its wastewater treatment processes (Rodríguez Furones and Ignacio Tejero Monzón 2023). Managing industrial wastewater comes with challenges because of the complexity and variability of effluents. Research into integrating blockchain technology in this field showcased the advantages of employing a ledger monitoring and recording treatment procedures. This innovative system enabled monitoring of waste quality and adherence to regulations and enhanced collaboration, among parties engaged in the treatment process (Bułkowska et al. 2023). Innovations in treatment technologies have played a role in tackling the issues surrounding wastewater management. One notable development is the creation of hybrid systems that merge biological treatment processes, with cutting-edge oxidation processes. These hybrid systems excel at treating wastewater with levels of pollutants more effectively leading to lower energy usage and enhanced treatment outcomes (Babuponnusami et al. 2023).

In context of wastewater, sustainability means finding ways to better manage wastewater in urban areas. IoT, AI, and blockchain are the technologies which can be used to tranform cities smart with efficient and transparent wastewater treatment and recycling systems.

10.4 Integration of Blockchain Technology in Water and Wastewater Management

10.4.1 Fundaments of Blockchain Technology

As we move from understanding the basics of smart water and wastewater management system, it is necessary to explore how blockchain technology can be integrated to make these systems even more stronger. Blockchain technology works as a decentralized ledger system which records all transactions across multiple computers so that the record cannot be altered retroactively. This immutable nature is secured with hashing and consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS) to ensure all nodes in the network come to an agreement on the status of ledgers (Nakamoto 2008).

The blockchain is advantageous in data security, transparency, and decentralization. These are very crucial features in water and wastewater management:

- *Data Security*: Blockchain technology uses advanced cryptographic techniques to secure data. All the transactions are encoded and connected to previous ones, which in turn makes it very difficult for any unauthorized entity to modify or tamper with the information. This feature is vital for preserving the accuracy of data, such as water quality measurements and customer usage details (Narayanan et al. 2016). Moreover, the decentralized nature of blockchain ensures there is no point of failure boosting the durability of data storage systems (Zheng et al. 2017).
- *Transparency*: The transparent ledger nature of blockchain ensures that all parties have the same information, leading to a great trust relationship between them (Xia et al. 2022). In water management, this transparency means water quality and usage metrics can be tracked in real time, enabling easy regulatory compliance and anomaly detection. For example, users and regulatory organizations may verify and validate water usage data stored on a blockchain, fostering trust (Owen 2023).
- *Decentralization*: The decentralized nature of blockchain eliminates the need for a single governing body, distributing control across the network. This minimizes the risk of centralized points of failure, and makes the system anti-fragile to attacks and failures (Swan 2015). Decentralization in water management implies a very robust and distributed distribution system where each node such as sensor and treatment plans can independently endorse and process transactions. Decentralization in water management leads to resilient and efficient distribution where

different entities work separately but together and validate and verify transactions (Xia et al. 2022).

10.4.2 Use Cases and Applications

Current and emerging use cases of blockchain in water management are

1. *Water Rights Trading*: Blockchain technology may facilitate a transparent and irreversible trading of water rights, guaranteeing fair and efficient distribution of the supply of water. A blockchain could record all transactions of water rights, providing the history of ownership and usage (Liu and Shang 2022). This promotes transparency among stakeholders, resolves conflicts, and provides for the equitable and correct distribution of water rights (Liu and Shang 2022). Additionally, smart contracts can also facilitate trading, performing operational work timely and in compliance with established regulations (Liu and Shang 2022; Satilmisoglu et al. 2024).
2. *Water Quality Monitoring*: Using blockchain and IoT sensors to monitor water quality in real time we can store the immutable and reliable data from sensors on the blockchain (Naqash et al. 2023; Satilmisoglu et al. 2024). This enhances transparency and accountability, as all the stakeholders can access and verify water quality data at any place and at any time (Satilmisoglu et al. 2024). For instance, blockchain can establish a transparent audit trail of water quality parameters after contamination, facilitating prompt identification and containment of the source and level of contamination (Zheng et al. 2017).
3. *Leak Detection and management*: Blockchain can contribute to greater assurance in the identification and control of leaks in water distribution systems. Smart contracts, for example, can trigger a response when an IoT sensor detects a leak, such as turning off the water supply or alerting maintenance workers (Naqash et al. 2023). As a consequence, the proactive strategy may decrease water loss, significantly improving the efficiency of water distribution networks. Furthermore, blockchain maintenance and leak response are recorded in the blockchain ledger (known as the immutable ledger in the blockchain) and can be audited (Xia et al. 2022).
4. *Billing and Payments*: Blockchain technology has the capability to optimize the billing process by promptly capturing real-time water consumption data, automatically creating invoices, and enabling secure payments using cryptocurrencies or tokens (Dogo et al. 2019). By recording all transactions and making them openly traceable, billing inconsistencies and fraud are minimized (Owen 2023). In addition, smart contracts can automate the payment procedure, guaranteeing punctual payments and diminishing administrative responsibilities.
5. *Regulatory Compliance*: Blockchain can be used to both comply with water management regulations and to protect the decentralized storage of this proof in a more secure fashion. Through a fully verifiable and transparent audit trail,

blockchains significantly reduce the risk of non-compliance and potential regulatory fines. For example, regulators can view a permanent history of water quality data, proving adherence to environmental regulations.

Examples of blockchain applications in wastewater treatment and monitoring are

6. *Effluent Quality Tracking*: By adopting this approach, the facility maintains a clear and easily traceable record for audits, ensuring compliance with the required discharge standards. Reinforcement of accountability leads to compliance with environmental regulations by treatment plants (Thakkar 2024). Effluent data may be recorded using blockchain technology to promptly detect any inconsistencies or violations by polluters, hence safeguarding the environment and public health (Khatri et al. 2021). Additionally, this data can also be shared with stakeholders such as regulatory bodies and the public, thus promoting trust and transparency (Sedlmeir et al. 2022).
7. *Asset Management*: Monitoring the lifecycle of wastewater treatment assets in the blockchain includes maintenance, repair, and performance data to improve operations and prolong the life of the asset. One of the functions of the system is to record all activities pertaining to assets to provide an audit trail (Thakkar 2024). As an example, creating a blockchain record for maintenance can tell you far in advance when your asset needs repair, improving the precision of the maintenance work, reducing downtime, and thereby improving operational efficiency. Blockchain is also transparent; this makes sure that all stakeholders have complete access to the same information and helps in making wise decisions and better allocation of resources (Xia et al. 2022).
8. *Decentralized Wastewater Systems*: Blockchain has the capability to enhance wastewater treatment systems through facilitating peer-to-peer engagements and transactions leading to increased efficiency and lowered infrastructure expenses (Sedlmeir et al. 2022). This approach enables smaller, community-based treatment systems to function more efficiently lessening the strain on centralized infrastructure and advocating for sustainable water management practices. The decentralized nature of blockchain guarantees that data and transactions are securely recorded and available, to all stakeholders involved, enhancing trust and accountability (2015).
9. *Rea-time Monitoring and Reporting*: Real-time data can be collected from wastewater systems through the secure exchange enabled by blockchains, which will speed up responses to potential issues as well as increase transparency in operations (Dogo et al. 2019). If sensors can keep a record of factors like pH level, temperature, or the concentration levels for different pollutants, this information can be stored on blockchain and accessed or reviewed in real time (Dogo et al. 2019). These monitoring systems help in identifying and solving the challenges, eventually leading to a reduction of environmental impact and an improvement of regulatory compliance (Liu and Shang 2022).
10. *Smart Contracting for Maintenance*: The automated scheduling based on blockchain in the smart contract has comprehensive application especially for maintenance of wastewater treatment plants and it helps to predict when

maintenance is required by intervening regularly resulting in an exact time-based prediction (Liu and Shang 2022). In addition, the immutable ledger of blockchain allows documentation for every maintenance operation which makes an audit and compliance check much easier (Liu and Shang 2022).

10.5 Role of IoT in Smart Water and Wastewater Management

IoT in water and wastewater management is the backbone of smart city applications. This system ensures real-time monitoring and data collection to utilize resource usage, diagnose quick problems at the source, and enhance the delivery of services. In this section, the impact of IoT technology on water and wastewater management will be discussed.

10.5.1 IoT Technologies and Sensors

Imagine a city where every single drop of water is counted, verified/validated as well as regulated. This vision is being accomplished by deploying IoT devices and sensors with blockchain-based solutions The use of IoT devices in water management covers a wide range:

- **Flow Sensors**: These are used to analyze the rate at which water flows through pipes and can help detect failures such as leaks or bursts swiftly.
- **Pressure Sensors**: These sensors help maintain the stability of a potable water supply system by identifying pressure drops that indicate leaks or pipe bursts. This helps in prompt repair, and water-wasting is minimized (Singh et al. 2023).
- **pH Sensors**: These sensors monitor pH levels of water, to make sure drinking water is safe and wastewater treatment works effeciently.
- **Turbidity Sensors**: They indicate how clear or clouded up water is becoming, which gives a fair estimate of its overall quality. Elevated turbidity levels may indicate the existence of contaminants or suspended particles that require treatment (Atlas Scientific 2022; YSI).
- **Chemical Sensors**: These sensors detect water contaminants and harmful substances to ensure safe drinking water and compliance with environmental law.

The data gathered by Internet of Things (IoT) devices in water management is extensive and diverse, serving as the foundation of smart water systems. This data consists of both quantitative and qualitative data that enable surveillance and evaluation as shown in Table 10.1.

Table 10.1 Types of data collected by IoT devices/sensors

Data type	Parameters	Description	Examples
Quantitative	Flow rates, pressure levels, temperature	Indentifiable variables to recognize patterns and anticipate issues	Tracking flow rates to predict obstacles
Qualitative	pH levels, turbidity, chemical composition	Evaluate the quality of water and ensure safety requlations (Chidiac et al. 2023)	Ensuring water quality safety with pH monitoring
Even	Leak detection, overflows, equipment failures	Information for managing incidents and responding to emergencies	Identifying leaks to avoid any potential damage

The integration of blockchain technology with the Internet of Things provides another degree of transparency and safety to data management, guaranteeing that data collected is tamper-proof and auditable (Naqash et al. 2023).

10.5.2 Data Collection and Real-Time Monitoring

IoT enables real-time monitoring that enhances urban water management. Imagine a network of sensors sending water quality and consumption data every second. This provides prompt identification of leaks, contamination, and unusual consumption patterns. Smart water networks use flow and pressure sensors to identify leaks quickly and reduce water loss (Hakak et al. 2020). City planners and utility administrators utilize dashboards to visualize real-time data for decision-making. Predictive analytics can use this data to forecast trends and strategize resource allocation and maintenance (Xia et al. 2022).

Cities like Singapore, Los Angeles, and Barcelona have already implemented IoT to enhance their water management. The smart water grid in Singapore has made significant contributions to sensing pipe leakage, water quality management, and pipeline failure prediction (Allen et al. 2012), proving its status as a worldwide model of urban water systems. A pilot project at the Los Angeles Department of Water and Power, using a Flume smart home water monitoring system, sends real-time water usage data to customers' cell phones, reducing waste and protecting water during drought conditions (Okoli and Kabaso 2024). A smart water management system based on IoT in Barcelona has achieved 25% less cost in water consumption after optimizing the irrigation of urban green spaces (wastewater management in a UN-water analytical brief 2017). After experiencing severe water scarcity from 2015 to 2018, Cape Town enforced strict water restrictions and used IoT to track water levels and usage, which allowed them to reduce water waste and distribute water efficiently. The collaborative approach averted "Day Zero" and turned the crisis around, restoring a sustainable level of water that provides important insights for other cities confronted by the same type of challenge (High Meadows Environmental Institute).

10.5.3 IoT in Wastewater Treatment

IoT devices are used in wastewater treatment from collection of wastewater to its disposal or reuse. The sensors measure key treatment parameters to ensure that the treated water satisfies regulatory/permit requirements to be released or reused safely.

- **Biological Oxygen Demand (BOD)**: This parameter measures the amount of organic matter in water. We use IoT sensors to track BOD levels, enhance biological treatment, and guarantee adherence to environmental regulations (Soetedjo et al. 2022).
- **Chemical Oxygen Demand (COD)**: These sensors measure the overall concentration of chemicals in the water, which helps to determine how well chemical treatment processes are performing (Soetedjo et al. 2022). Real-time data allows for the adjustment of chemical dosages to attain the necessary treatment concentrations.
- **Total Suspended Solids (TSS)**: The sensors are responsible for keeping track of the solid particles in wastewater. Elevated levels of suspended solids may suggest problems with the treatment process that require immediate attention.
- **Ammonia and Nitrate Levels**: These metrics serve as signs of pollution and are closely monitored to prevent eutrophication in bodies of water where they flow. IoT sensors offer up-to-the-minute information, enabling the management of removal procedures (Xia et al. 2022).

IoT sensors send real-time data to operators, allowing them to control the treatment process dynamically and optimize performance. This assures regulatory compliance and improves treatment efficiency, lowering operational costs (Alzahrani et al. 2023). Dubai, Miami Dade County, and Jeddah have adopted these technology solutions for managing wastewater, improving efficiency, and promoting sustainability. Miami-Dade County uses real-time data from Itron to enhance water quality and address challenges (Blackman 2020). In Dubai, the Smart Dubai initiative utilizes sensors to oversee water quality, identify leaks, and control treatment procedures. To incentivize wastewater recycling, Jeddah employs a blockchain-powered IoT-based wastewater management system, leading to increased recycling rates and supporting sustainable water management within the city. These innovative wastewater management approaches align with the Emirates sustainability objectives (AlGhamdi and Sharma 2022).

While the advantages are many, the adoption of IoT in water and wastewater management comes with challenges. One of the core tasks lies in the secure storage of data collected via IoT devices. This can be effectively solved using blockchain technology securing the data transmission and storage with encryption requiring secure provisions over the data integrity and transparency rendering blockhain a perfect solution for the security of the IoT data (Eghmazi et al. 2024; Cui et al. 2019). Many water management systems are built on very old infrastructure and in such cases the integration with legacy systems is a challenge in itself. For effective roll-out, hybrids that connect the old with new technology are required and middleware platforms can help in communication between legacy systems and modern IoT devices (Amaral et al. 2016). In addition, the huge amount of data collected by IoT devices needs resilient data management and analytics solutions. Blockchain technology can improve data management by offering secure, transparent, and decentralized data processing, while powerful machine learning algorithms analyze and derive practical insights from the data. Cloud computing technologies can efficiently manage massive datasets by offering scalable storage and processing power (Naghib et al. 2022).

10.6 Machine Learning for Data Analysis and Predictive Maintenance

10.6.1 Machine Learning in Water Management

Machine learning (ML) is a field of artificial intelligence that specifically focuses on developing and analyzing statistical algorithms capable of learning from data and make informed decisions. ML can be used for monitoring big data in water management, examining extensive datasets, optimizing operations, predicting system failures as well as yielding efficient water supply and wastewater treatment systems (Ghobadi and Kang 2023; Zhang and Ng 2024).

Below are the ML techniques that are of significant use in the water and wastewater management:

- **Supervised Learning**: In this technique, we use datasets with labels to train the algorithms for detecting patterns and predicting the results. We can use it to predict water demand by analyzing consumption history (Bata et al. 2020).
- **Unsupervised Learning**: This method focuses on unlabeled data in order to discover well-kept patterns and relationships. Clustering segments common patterns of usage and therefore partitions into different water consumption profiles and enhances resource allocation (Ghobadi and Kang 2023; Laspidou et al. 2015).
- **Reinforcement Learning**: It is a process in which we train the algorithms to take a set of decisions in order by rewarding useful behaviors. This method is used to control dynamic systems such as the management of water distribution networks to save energy and reduce costs (Essamlali et al. 2024).

10.6.2 Predictive Analytics and Maintenance

These models are trained with data collected from sensors using ML methods to predict when devices are likely to fail or need service. This proactive approach has successfully reduced the downtime of systems, lengthened the life of infrastructure, and also results in cost-saving from expensive repair work (Kane et al. 2022).

ML algorithms have been successfully used by urban utilities to predict pump failures and hence schedule maintenance in a timely manner, therefore preventing the systems from failing with costly consequences. In a case study, these algorithms were 90% accurate at predicting water pump failures, so timely maintenance could be conducted and avoid costly breakdown (Chhabria et al. 2022; Tyralis et al. 2019). The implementation of predictive maintenance strategies to water management systems will enable these assets reliable and optimized (Kane et al. 2022), contributing with the sustainability aspects inherent to this type of resource.

10.6.3 Data-Driven Decision-Making

As far as water resource management is concerned, ML techniques would be helpful because these algorithms can handle a massive amount of data and produce actionable outputs in the form of decision trees or random forest algorithms (Ghobadi and Kang 2023; Vallejo-Gómez et al. 2023). These smart irrigation algorithms are used in smart plants for water usage, plant scheduling, and predicting losses of water which are automatic, based on soil moisture and meteorological predictions (Erokhin et al. 2024). Also, by using ML-based decision-making strategies in treatment plants and water savings sustainability can be enhanced (Guo et al. 2024).

10.7 Case Studies and Real-World Implementations

We have also seen the positive outcome in a number of case studies for application of blockchain technology in smart water systems and sustainable wastewater management. The following section will present key cases of implementation that demonstrated proven success factors and informing examples.

10.7.1 Successful Implementations of Blockchain in Water and Wastewater Management

Applications of blockchain technology in water management systems have enabled to address some major problems like data integrity, transparency, and efficiency. Seosan City in South Korea has introduced a blockchain-based water management system to improve efficiency and transparency. It authenticates data on smart water meter sensors and stores this information on blockchain ensuring accuracy, security, and tamper-proofing property (Sitanggang et al. 2023). The blockchain system communicates with IoT sensors which monitor the water quality and usage in real time without any effort. Advanced ML algorithms are then used to analyze the data collected and predict if there are likely any issues ahead (leaks and pollution) (Sitanggang et al. 2023). Barcelona makes use of blockchain, machine learning, and IoT to take control over its water infrastructure with an integrated water management system. The system ensemble uses many IoT sensors to collect and share data all the time like water prussure, rate of flow, and water quality indicator. These data are stored by blockchain technology through encryption, such that the integrity of it is preserved and swift access is enabled to register stakeholders online (Poberezhna 2019).

10.7.2 Analysis of the Benefits and Challenges of These Integrated Approaches

Benefits:

- **Data Integrity and Security**

Concerning data, blockchain ensures that IoT devices collect unalterable and secure information boosting stakeholder faith in it, which improves the accuracy and reliability in water management while mitigating tampering risks and establishing trust among stakeholders.

- **Accountability**

This has increased transparency through a traceable ledger and helped build public trust, which is critical to maintaining compliance as well holding people responsible.

- **Real-time Monitoring and Predictive Maintenance**

The projected maintenance schedule offered by the refined ML algorithms can efficiently reduce operational expenses, minimize downtime, and increase effectiveness in maintaining it.

- **Enhanced Regulatory Compliance**

Improved regularity compliance with blockchain records that ensure water quality and data usage are accurate, transparent, and accessible so we meet local or international needs easily.

- **Resource Optimization**

In water treatment, ML has enabled lead detction and more efficient resource allocation in places like Barcelona (less wasted water) and Singapore (better energy management).

Challenges:

- **Integration Complexity**

Integration of technologies, blockchain, ML, and IoT constitutes a process that is already complex on their own and they integrate one another. It may result in additional intricacies leading to elongated implementation periods with cost increaments.

- **Scalability**

Blockchain technology, on the other hand, is known for its scalability. Thus, IoT devices rely heavily on blockchain in their data and traffic operation management. Scalability though remains a big challenge for these devices and needs further improvements.

- **Data Privacy**

But it is also the case that data protection laws require sensitive information to be protected and not visible on a blockchain or must be exchangeable in an anonymized form only.

- **Cost**:

Some regions may be financially constrained and thus struggle to fund rolling out an integrated system to achieve cost savings.

- **Interoperability**

One of the most challenging tasks in the integration of these technologies is interoperating it with other systems. The smart city ecosystem, whose protocols and interfaces are still being standardized.

10.8 Challenges and Future Directions

10.8.1 Technical Challenges

However, there is a range of technical challenges in implementation with blockchain and ML as well as IoT for water and wastewater management. Among these, the three primary concerns are scalability, interoperability, and security.

IoT-based smart water management systems will generate massive data, and hence scalability is a big issue. Although blockchain technology ensures the security and immutability of information, it is less efficient at handling and storing massive volumes of data. Current research emphasizes the implementation of scalability in water management applications through techniques such as sharding and off-chain solutions. However, despite their potential, these methods remain largely unimplemented (Rodríguez Furones and Ignacio Tejero Monzón 2023). The challenge in real-time water monitoring and response systems may be the optimization of those solutions, requiring a specific approach.

Another significant challenge is interoperability. Incompatibility results from the integration of disparate systems and technologies involved, each residing on their own incompatible protocols and standards. We should implement standard protocols to ensure smooth data exchange among IoT devices, ML algorithms, and blockchain platforms. While current research is focused on developing interoperable frameworks and middleware solutions to address these gaps, the comprehensive, universally accepted standards for them are in the final stages (Xie et al. 2019).

If the systems we are using handle sensitive information, security should be our top priority. The security stakes are high for IoT devices; they hold one of the primary avenues for cyber-attackers to skew data. Although blockchain is inherently secure, it is still vulnerable to threats like 51% attacks or Sybil attacks. Studies suggest that the combination of blockchain technology, improved encryption methods, and secure IoT frameworks can help reduce these dangers. However, the adoption of these solutions on a large scale is still ongoing (Adhikari and Ramkumar 2023).

10.8.2 Regulatory and Compliance Challenges

The implementation of blockchain, Internet of Things (IoT), and machine learning (ML) technologies in water management not only poses technical difficulties but also involves regulatory challenges. Either the legal and regulatory frameworks do not account for the growth of new technological capabilities, or when they do, these novel possibilities prove difficult to implement. One major challenge is ensuring compliance with existing standards and regulations. For example, data privacy laws like GDPR are subject to stringent regulations regarding both data collection, storage, and sharing. However, the immutability of the blockchain directly contradicts these regulations, as this same feature prevents the alteration and deletion of data to comply with privacy requests (Samanta and Sarkar 2023; Bernardi 2019). Researchers are currently focusing on developing blockchain designs that adhere to privacy regulations and safeguard data integrity (Belen-Saglam et al. 2023). Ensuring compliance with local and international environmental regulations can be challenging, especially when employing cutting-edge technologies that regulators may have limited understanding of. To tackle this challenge, ongoing communication among tech experts, water management entities, and regulatory agencies is vital for crafting protocols and benchmarks (Muriuki 2024).

10.8.3 Future Developments and Research Areas

Future studies in the field of technology for sustainable smart water and wastewater management should prioritize scalability solutions and the integration of advanced machine learning. Enhancing scalability is essential to managing the volumes of data generated by IoT devices in water management systems. Research is underway on sharding, off-chain transactions, and Layer 2 solutions to boost the blockchain's capability for real-time monitoring and management of water (Rodríguez Furones and Ignacio Tejero Monzón 2023). Also, the integration of blockchain along with more advanced machine learning algorithms can improve the maintenance and operational efficiency of water management systems. This approach may be extended to develop machine learning models, by leveraging the transparent data storage of blockchains, for improved analytics in leak detection, equipment failure prediction, and water distribution network optimization (Naqash et al. 2023).

Emerging Technologies and Their Potential Impact:

Water management systems may further be significantly driven by advanced technologies, e.g., quantum computing, edge computing, 5G, etc. In theory, the technology could give networks a superpower that would allow them to solve complex optimization problems in an incredibly short time. The impacts of this include potential improvements in water resource management, reliable predictive modeling, and immediate decision-making (Chhabria et al. 2022). Combining edge computing with 5G technology may also contribute to the improvement of blockchain-based water management effectiveness and responsiveness by reducing latency as well as supporting real-time analysis (Chhabria et al. 2022).

Socio-Economic Impacts:

The area of water management has social and economic implications when integrating blockchain along with IoT and ML. The innovations can improve water use efficiency while promoting the sustainability of implications for savings to cities and people as well as environmental benefits. Still, the costs of implementing technology upfront can make it difficult for low-income areas to adopt. In addition, the shift to technology-driven water management systems may have consequences for those employed in some roles. To harness the promise for sustainable urban water management of those technologies, research will need to be continued and development-oriented regulation as well as socio-econimic reflection should stay in focus.

10.9 Conclusion

In this chapter, the possibilities of revolutionizing sustainable smart water and wastewater management through blockchain technology along with IoT and ML were explored. Together with blockchain's ability to provide a reliable medium for managing data integrity and resources, IoT enabled real-time monitoring as well as predictive analysis and optimizations of systems by ML algorithms, and we have seen that these technologies can significantly enhance the water management efficiency and minimize its wastage alongside assisting it in fostering sustainable practices within smart cities. The contrivance of the blockchain, IoT, and ML into watering systems will be a tributary to urban infrastructure. Using these technologies, the cities can combat growing challenges from water stress and pollution, enhance the reliability and quality of their service levels in this essential area, achieving environmental as well as economic benefits. In conclusion, sustainable urban evolution necessitates challenges rooted within complexities and integrated regulations of socio-economic barriers. Utilizing the innovative technologies as well as engaing with all parties involved is essential to conquer these barriers that will meet the demands not only for this generation, but for future generations as well.

References

Adhikari N, Ramkumar M (2023) IoT and blockchain integration: applications, opportunities, and challenges. Network 3(1):115–141. https://doi.org/10.3390/network3010006

AlGhamdi R, Sharma SK (2022) IoT-based smart water management systems for residential buildings in Saudi Arabia. Processes 10(11):2462. https://doi.org/10.3390/pr10112462

Allen M, Preis A, Iqbal M, Whitttle A (2012) Case study: a smart water grid in Singapore. Water Pract Technol 7

Alzahrani AIA, Chauhdary SH, Alshdadi AA (2023) Internet of Things (IoT)-based wastewater management in smart cities. Electronics 12(12):2590. https://doi.org/10.3390/electronics12122590

Amaral LA, de Matos E, Tiburski RT, Hessel F, Lunardi WT, Marczak S (2016) Middleware technology for IoT systems: challenges and perspectives toward 5G. In: Modeling and optimization in science and technologies, pp 333–367, January 2016. https://doi.org/10.1007/978-3-319-30913-2_15

Babuponnusami A et al (2023) Advanced oxidation process (AOP) combined biological process for wastewater treatment: a review on advancements, feasibility and practicability of combined techniques. Environ Res 237:116944–116944. https://doi.org/10.1016/j.envres.2023.116944

Bata M, Carriveau R, Ting DS-K (2020) Short-term water demand forecasting using hybrid supervised and unsupervised machine learning model. Smart Water 5(1). https://doi.org/10.1186/s40713-020-00020-y

Belen-Saglam R, Altuncu E, Lu Y, Li S (2023) A systematic literature review of the tension between the GDPR and public blockchain systems. Blockchain: Res Appl 4(2):100129. https://doi.org/10.1016/j.bcra.2023.100129

Bernardi SDC (2019) Blockchain and GDPR. Blockchain Compliance White Paper, January 2019. https://www.academia.edu/41182764/Blockchain_and_GDPR. Accessed 11 June 2024

Blackman J (2020) Miami-dade deploys IoT solution from Itron for waste water management. RCR Wireless News, 28 May 2020. https://www.rcrwireless.com/20200528/internet-of-things/miami-dade-deploys-iot-solution-from-itron-for-waste-water-management. Accessed 04 June 2024

Bułkowska K, Zielińska M, Bułkowski M (2023) Implementation of blockchain technology in waste management. Energies 16(23):7742. https://doi.org/10.3390/en16237742

Campbell C, Greenberg R, Mankikar D, Ross R (2016) A case study of environmental injustice: the failure in flint. Int J Environ Res Public Health 13(10):951. https://doi.org/10.3390/ijerph13100951

Chhabria S, Ghata R, Mehta V, Ghosekar A, Araspure M, Pakhide N (2022) Predictive maintenance using machine learning on industrial water pumps. Int J Innov Eng Sci 7(9):76–81. https://doi.org/10.46335/ijies.2022.7.9.16

Chidiac S, El Najjar P, Ouaini N, El Rayess Y, El Azzi D (2023) A comprehensive review of water quality indices (WQIs): history, models, attempts and perspectives. Rev Environ Sci Bio/Technol 22. https://doi.org/10.1007/s11157-023-09650-7

Cui P, Guin U, Skjellum A, Umphress D (2019) Blockchain in IoT: current trends, challenges, and future roadmap. J Hardw Syst Secur 3:338–364. https://doi.org/10.1007/s41635-019-00079-5

Dada MA et al (2024) Review of smart water management: IoT and AI in water and wastewater treatment. World J Adv Res Rev 21(1):1373–1382. https://doi.org/10.30574/wjarr.2024.21.1.0171

Dogo EM, Salami AF, Nwulu NI, Aigbavboa CO (2019) Blockchain and Internet of Things-Based Technologies for Intelligent Water Management System. Artif Intell IoT 129–150. https://doi.org/10.1007/978-3-030-04110-6_7

Eghmazi A, Ataei M, Landry Jr R, Chevrette G (2024) Enhancing IoT data security: using the blockchain to boost data integrity and privacy. IoT 5(1):20–34. https://doi.org/10.3390/iot5010002

Erokhin V, Mouloudj K, Bouarar AC, Mouloudj S, Gao T (2024) Investigating farmers' intentions to reduce water waste through water-smart farming technologies. Sustainability 16(11):4638–4638. https://doi.org/10.3390/su16114638

Essamlali I, Nhaila H, El Khaili M (2024) Advances in machine learning and IoT for water quality monitoring: a comprehensive review. Heliyon 10(6):e27920–e27920. https://doi.org/10.1016/j.heliyon.2024.e27920

Farooqi AM, Hassan SI, Afshar Alam M (2019) Sustainability and fog computing: applications, advantages and challenges, February 2019. https://doi.org/10.1109/iccct2.2019.8824983

Ghobadi F, Kang D (2023) Application of machine learning in water resources management: a systematic literature review. Water 15(4):620–620. https://doi.org/10.3390/w15040620

Guo H, Liu X, Zhang Q (2024) Identifying daily water consumption patterns based on k-means clustering, agglomerative hierarchical clustering, and spectral clustering algorithms. Aqua 73(5). https://doi.org/10.2166/aqua.2024.294

Hakak S, Khan WZ, Gilkar GA, Haider N, Imran M, Alkatheiri MS (2020) Industrial wastewater management using blockchain technology: architecture, requirements, and future directions. IEEE Internet of Things Mag 3(2):38–43. https://doi.org/10.1109/iotm.0001.1900092

How cape town defeated day zero: winning community compliance with water restrictions in an emergency. High Meadows Environmental Institute. https://environment.princeton.edu/research/grand-challenges-overview/urban-grand-challenge/how-cape-town-defeated-day-zero-winning-community-compliance-with-water-restrictions-in-an-emergency/

Kane AP, Kore AS, Khandale AN, Nigade SS, Joshi PP (2022) Predictive maintenance using machine learning, 19 May 2022. https://arxiv.org/abs/2205.09402. Accessed 05 June 2024

Kavya M, Mathew A, Shekar PR, Sarwesh P (2023) Short term water demand forecast modelling using artificial intelligence for smart water management. Sustain Cities Soc 95:104610. https://doi.org/10.1016/j.scs.2023.104610

Khatri S, Alzahrani FA, Ansari MTJ, Agrawal A, Kumar R, Khan RA (2021) A systematic analysis on blockchain integration with healthcare domain: scope and challenges. IEEE Access 9:84666–84687. https://doi.org/10.1109/access.2021.3087608

Laspidou C, Papageorgiou E, Kokkinos K, Sahu S, Gupta A, Tassiulas L (2015) Exploring patterns in water consumption by clustering. Procedia Eng 119(1877–7058):1439–1446. https://doi.org/10.1016/j.proeng.2015.08.1004

Liu Y, Shang C (2022) Application of blockchain technology in agricultural water rights trade management. Sustainability 14(12):7017. https://doi.org/10.3390/su14127017

Lowe M, Qin R, Mao X (2022) A review on machine learning, artificial intelligence, and smart technology in water treatment and monitoring. Water 14(9):1384. https://doi.org/10.3390/w14091384

Muriuki W (2024) Blockchain and GDPR: navigating privacy regulations. Total Bitcoin, 17 February 2024. https://totalbitcoin.org/blockchain-gdpr/. Accessed 11 June 2024

Naghib A, Jafari Navimipour N, Hosseinzadeh M, Sharifi A (2022) A comprehensive and systematic literature review on the big data management techniques in the internet of things. Wirel Netw. https://doi.org/10.1007/s11276-022-03177-5

Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system, October 2008. https://bitcoin.org/bitcoin.pdf. Accessed 26 May 2024

Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S, Clark J (2016) Bitcoin and cryptocurrency technologies introduction to the book. https://www.lopp.net/pdf/princeton_bitcoin_book.pdf

Naqash MT, Syed TA, Alqahtani SS, Siddiqui MS, Alzahrani A, Nauman M (2023) A blockchain based framework for efficient water management and leakage detection in urban areas. Urban Sci 7(4):99. https://doi.org/10.3390/urbansci7040099

Okoli NJ, Kabaso B (2024) Building a smart water city: IoT smart water technologies, applications, and future directions. Water 16(4):557. https://doi.org/10.3390/w16040557

Owen DL (2023) Smart water management. River. https://doi.org/10.1002/rvr2.29

Poberezhna A (2019) Addressing water sustainability with blockchain technology and green finance. Elsevier eBooks, no. 9780128144473, pp. 189–196, January 2018. https://doi.org/10.1016/b978-0-12-814447-3.00014-8

PUB (2018) Innovation in water, Singapore. PUB, Singapore's National Water Agency, Singapore. www.pub.gov.sg/research. Accessed 02 June 2024

Radcliffe JC, Page D (2020) Water reuse and recycling in Australia-history, current situation and future perspectives. Water Cycle 1(1):19–40. https://doi.org/10.1016/j.watcyc.2020.05.005

Rodríguez Furones A, Ignacio Tejero Monzón J (2023) Blockchain applicability in the management of urban water supply and sanitation systems in Spain. J Environ Manag 344:118480. https://doi.org/10.1016/j.jenvman.2023.118480

Rodríguez Furones A, Ignacio Tejero Monzón J (2023) Blockchain applicability in the management of urban water supply and sanitation systems in Spain. J Environ Manag 344(0301–4797):118480. https://doi.org/10.1016/j.jenvman.2023.118480

Samanta S, Sarkar A (2023) IoT and blockchain for smart water quality management in future cities: a hyperledger fabric framework for smart water quality management and distribution. Research Square, 12 December 2023. https://www.researchsquare.com/article/rs-3727101/v1. Accessed 02 June 2024

Satilmisoglu TK, Sermet Y, Kurt M, Demir I (2024) Blockchain opportunities for water resources management: a comprehensive review. Sustainability 16(6):2403. https://doi.org/10.3390/su16062403

Sedlmeir J, Lautenschlager J, Fridgen G, Urbach N (2022) The transparency challenge of blockchain in organizations. Electron Mark 32. https://doi.org/10.1007/s12525-022-00536-0

Singh A-T, Eskenazi A, Kort M, Vanduwin R, Wageningen S, Blockchain and IoT for drinking water: a game-changing opportunity or a risky proposition. https://sdgs.un.org/sites/default/files/2023-05/A46%20-%20Singh%20-%20Blockchain%20and%20IoT%20for%20water%20A%20Game-Changing%20Opportunity.pdf

Singh BJ, Chakraborty A, Sehgal R (2023) A systematic review of industrial wastewater management: evaluating challenges and enablers. J Environ Manag 348:119230. https://doi.org/10.1016/j.jenvman.2023.119230

Sitanggang RV, Ruttenberg F, Singh A-T (2023) Blockchain and iot for drinking water in G20 countries: a game- changing opportunity

Soetedjo A et al (2022) Real-time implementation of wastewater monitoring system on the communal wastewater treatment plant using the iot technology. IOP Conf Ser Earth Environ Sci 1030(1):012006–012006. https://doi.org/10.1088/1755-1315/1030/1/012006

Swan M (2015) Blockchain: blueprint for a new economy. O'Reilly Media, Inc. https://books.google.co.in/books?id=RHJmBgAAQBAJ&pg=PA47&source=gbs_selected_pages&cad=1#v=onepage&q&f=true. Accessed 03 June 2024

Tajudin MK, Sarijari MA, Rashid RA (2024) Blockchain-based internet of thing for smart river monitoring system. In: IOP conference series: materials science and engineering. IOP Publishing Ltd. https://iopscience.iop.org/article/10.1088/1757-899X/884/1/012082. Accessed 02 June 2024

Thakkar DS et al (2024) Blockchain-orchestrated intelligent water treatment plant profiling framework to enhance human life expectancy. IEEE Access 12:49151–49166. https://doi.org/10.1109/access.2024.3384607

The World Bank (2019) Overview. World Bank. https://www.worldbank.org/en/topic/water/overview. Accessed 02 June 2024

Tyralis H, Papacharalampous G, Langousis A (2019) A brief review of random forests for water scientists and practitioners and their recent history in water resources. Water 11(5):910. https://doi.org/10.3390/w11050910

United Nations (2022) Water – at the center of the climate crisis. United Nations. https://www.un.org/en/climatechange/science/climate-issues/water

United Nations (2023) UN conference seeks solutions to global water crisis. UN News, 22 March 2023. https://news.un.org/en/story/2023/03/1134887. Accessed 16 May 2024

United Nations (2023) Don’t let wastewater opportunities flow down the drain|UN News. news.un.org, 23 August 2023. https://news.un.org/en/story/2023/08/1140002. Accessed 26 May 2024

U. N. D. of E. and S. A. (UN D.) United Nations, 2018 revision of world urbanization prospects. United Nations, 16 May 2018. https://www.un.org/en/desa/2018-revision-world-urbanization-prospects. Accessed 26 May 2024

Vallejo-Gómez D, Osorio M, Hincapié CA (2023) Smart irrigation systems in agriculture: a systematic review. Agronomy 13(2):342. https://doi.org/10.3390/agronomy13020342

Wastewater management a UN-water analytical brief analytical brief. https://www.unwater.org/sites/default/files/app/uploads/2017/05/UN-Water_Analytical_Brief_Wastewater_Management.pdf

What is a turbidity sensor? Atlas Scientific, 13 May 2022. https://atlas-scientific.com/blog/what-is-a-turbidity-sensor/#:~:text=Turbidity%20sensors%20are%20a%20piece. Accessed 04 June 2024

World Bank (2016) The world bank and the international water association to establish a partnership to reduce water losses. World Bank, 01 September 2016. https://www.worldbank.org/en/news/press-release/2016/09/01/the-world-bank-and-the-international-water-association-to-establish-a-partnership-to-reduce-water-losses. Accessed 26 May 2024

Xia W, Chen X, Song C (2022) A framework of blockchain technology in intelligent water management. Front Environ Sci 10. https://doi.org/10.3389/fenvs.2022.909606

Xie J, Yu FR, Huang T, Xie R, Liu J, Liu Y (2019) A survey on the scalability of blockchain systems. IEEE Netw 33(5):166–173. https://doi.org/10.1109/mnet.001.1800290

YSI, Turbidity measurement and monitoring in water quality analysis|YSI. www.ysi.com, https://www.ysi.com/parameters/turbidity

Zhang W, Ma F, Ren M, Yang F (2021) Application with Internet of things technology in the municipal industrial wastewater treatment based on membrane bioreactor process. Appl Water Sci 11(3). https://doi.org/10.1007/s13201-021-01375-8

Zhang H, Ng C (2024) Applications of artificial intelligence, machine learning, and data analytics in water environments. ACS ES & T Water 4(3):761–763. https://doi.org/10.1021/acsestwater.4c00140

Zheng Z, Xie S, Dai H, Chen X, Wang H (2017) An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE international congress on big data (bigdata congress), Honolulu, HI, USA, pp 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

Zulkifli CZ et al (2022) IoT-based water monitoring systems: a systematic review. Water 14(22):3621. https://doi.org/10.3390/w14223621