

Debashis De
Siddhartha Bhattacharyya
Joel J. P. C. Rodrigues *Editors*

Blockchain based Internet of Things

Lecture Notes on Data Engineering and Communications Technologies

Volume 112

Series Editor

Fatos Xhafa, Technical University of Catalonia, Barcelona, Spain

The aim of the book series is to present cutting edge engineering approaches to data technologies and communications. It will publish latest advances on the engineering task of building and deploying distributed, scalable and reliable data infrastructures and communication systems.

The series will have a prominent applied focus on data technologies and communications with aim to promote the bridging from fundamental research on data science and networking to data engineering and communications that lead to industry products, business knowledge and standardisation.

Indexed by SCOPUS, INSPEC, EI Compendex.

All books published in the series are submitted for consideration in Web of Science.

More information about this series at <https://link.springer.com/bookseries/15362>

Debashis De · Siddhartha Bhattacharyya ·
Joel J. P. C. Rodrigues
Editors

Blockchain based Internet of Things

Editors

Debashis De
Department of Computer Science
and Engineering
Maulana Abul Kalam Azad University
of Technology
West Bengal, India

Siddhartha Bhattacharyya
Rajnagar Mahavidyalaya
Birbhum, India

Joel J. P. C. Rodrigues 
College of Computer Science
and Technology
China University of Petroleum (East China)
Qingdao, China

Research, Development and Innovation
Senac Faculty of Ceará
Fortaleza-CE, Brazil

Covilhã Delegation
Instituto de Telecomunicações
Covilhã, Portugal

ISSN 2367-4512

ISSN 2367-4520 (electronic)

Lecture Notes on Data Engineering and Communications Technologies

ISBN 978-981-16-9259-8

ISBN 978-981-16-9260-4 (eBook)

<https://doi.org/10.1007/978-981-16-9260-4>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2022

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

*Debashis would like to dedicate this volume
to his beloved father Late Sir Dilip Kimar De.*

*Siddhartha would like to dedicate this volume
to Ben Reeves, the founder of Blockchain.info.*

*Joel would like to dedicate this volume to his
wife Charlene and his lovely sons Catarina,
José and Carolina.*

Preface

Blockchain is an efficient, transparent, highly secured platform for data transaction. It consists of growing number of transaction records or blocks which are linked via cryptographic hash values. Each block contains data, own hash value, hash value of next block, and nonce value. Any node/workstation from any geographical location can participate in blockchain platform. Communications between nodes are managed by various cryptographic protocols. Blockchain as a platform has emerged as one of the decisive expertise with applications across various industrial domains. It is known to be a highly secured platform with real-time notification to provide the property of transparency to all the stake holders. The objective of the book is to update recent advancements on blockchain as a platform with incorporation of properties of Artificial Intelligence.

Companies around the world have a close look on the exponential advancements of blockchain and IoT technology. A Gartnet study in 2018 reveals that blockchain is going to add \$3.1 trillion in business value by 2030. Another study by Forbes in 2017 analyzed the global IoT market to expect growth from \$157 B in 2016 to \$457 B by 2020. Thus, a lot of advancements of both the technologies to happen in near future what we could really imagine.

Intelligent blockchain as a platform will ensure trust through technology among participating organizations unlike existing contracts. This change is already apparent in variety of industries including healthcare, supply chain, finance, manufacturing, etc.

IoT ecosystems suffer heavily due to a number of security issues. A huge amount of data, devices are getting hacked. As an example in healthcare system, monitoring of patient's real-time data is getting increased day by day and entry points of intruders also increase. These are critically important data and need to be nurtured with utmost care. Blockchain as a platform completely eliminates any chance of misuse of those paramount data.

The proposed book is aimed to introduce the basic operating principle and fundamentals of blockchain technology. The contributory chapters will focus on the limitations of the state-of-the-art blockchain use cases and propose methods of elimination. The use of blockchain framework for IoT systems would also be highlighted

with recourse to specific IIoT application areas like social networking, decentralized autonomous organizations, energy, smart grid, logistics, transportation, supply chain, monetization, e-business, notarization, e-government, healthcare, commerce, insurance, finance, banking, education, learning, crowdsourcing, and crowd sensing.

This volume comprises 12 well versed chapters on the fundamentals of the blockchain technology with reference to Internet of Things encompassing different application domains.

Industry 5.0 is a new dawn in massive automated production based on the active collaboration between the creative potential of people and accurate apparatuses. Internet of Things (IoT) can make environments smarter, increasingly connected, more profitable and efficient by connecting many distributed and ubiquitously available intelligent devices and sensors through multi-level communication infrastructures. While this should ideally map to a decentralized hardware and software platform, current solutions are mostly based on centralized infrastructures, with many disadvantages, e.g., high maintenance costs, low interoperability, single point of failure, etc. An additional challenge in supporting decentralization is achieving distributed consensus among autonomous IoT objects. In this view, blockchain represents a promising solution for enabling a decentralized IoT framework. However, due to the heterogeneity, IoT requires addressing several additional challenges, including ensuring scalability, interoperability, security, privacy, and efficiency. Chapter “[BCoT: Introduction to Blockchain-Based Internet of Things for Industry 5.0](#)” introduces the integration of blockchain technology with the Internet of Things to connect everything globally.

Majority of interaction in an IoT (Internet of Things) ecosystem occurs via machine-to-machine interactions. As a result, establishing confidence among the participating equipment is a significant challenge, particularly given the fact that IoT technology has not been adequately addressed. The blockchain enables autonomous smart devices and completely removes the need for intermediary parties. However, since blockchain enables increased scalability, security, dependability, and privacy, it can function as a catalyst in this area. This may be accomplished by utilizing blockchain technology to monitor and utilize billions of devices connected to IoT ecosystems in order to facilitate and/or coordinate transaction processing. By eliminating a single point of failure, the implementation of blockchain in the IoT ecosystem will also improve reliability. The cryptographic algorithms are used to encrypt the block data, and the hashing techniques can provide additional security. Chapters “[Blockchain-Based Internet of Things: Challenges and Opportunities](#)” and “[Challenges and Issues in Blockchain-Based IoT Services](#)” put forward several perspectives of the challenges and problems encountered in Blockchain (BC)-based Internet of Things (IoT) applications, while considering IoT as a unique solution.

Cyber-Physical System (CPS) enables to combine the physical objects with computing and storage capabilities to have data exchange in an interconnected network of systems and objects. Blockchain is a recently distributed computing paradigm which provides a promising solution for modern CPS application. It forms an underpinning technique for CPS that offers strong added value to Industrial IoT (IIoT), fault-tolerant, reliable, secure, and efficient computing infrastructure. The

inherent integration of consensus algorithms and distributed storage with advanced security protocols provide powerful solutions for CPS applications. Blockchains in CPSs/IoT ensure secure and saved information for different industrial applications and achieve a means of adaptability, process, and operation protection, for example, in manufacturing, transportation, healthcare, and energy applications. Chapter “[Blockchain for IoT-Based Cyber-Physical Systems \(CPS\): Applications and Challenges](#)” provides an extensive technical background for blockchain in IoT-based CPS. Applications, opportunities, and challenges as far as the combination of CPS, IoT, and blockchain are concerned.

Since the boom of 2009 sparked by Bitcoin, blockchain has hardly left any field untouched. Blockchain has been countered by the lack of interoperability between different protocols. Privacy and identity management in the distributed ledger technologies have immense potential. These two areas of blockchain have seen steady progress and innovation. In chapter “[Blockchain in IoT and Beyond: Case Studies on Interoperability and Privacy](#)”, the authors start by first discussing recent works of blockchain and allied technologies in the field of IoT with a focus on how such works can serve as a basis for the next generation of amalgamated solutions. The authors also put forward a short survey of blockchain in IoT and IIoT followed by proof of concepts of distributed ledger technology used in literature. Then the chapter provides a discussion on distributed identity management with zero knowledge proof followed by self-sovereign identity. Subsequently, a detailed case study of Hyperledger Indy is presented. Finally, the authors also illustrate a case study involving the interoperability issue and contemporary survey of Polkadot.

Due to high growth of Internet of Things and cloud computing services, it has brought great changes within the human lifestyle in the various fields such as medical, agricultural, educational, military, environmental, etc. So, it is necessary to understand the building blocks basic of the Internet of Things and identifying weaknesses and data security of user. Blockchain plays an important role in the implementation of security aspects in cloud computing. In chapter “[Hybrid Blockchain-Enabled Security in Cloud Storage Infrastructure Using ECC and AES Algorithms](#)”, the authors have analyzed the security aspects of data stored in the cloud through hybrid security system enabled with blockchain technology using cryptographic algorithms like ECC and AES. The proposed framework is found to exhibit higher security with more efficiency than others.

The introduction of Blockchain Technology (BT) has evolved into a distinctive, disturbing, and trendy technology in recent years. Data security and privacy are prioritized in BT’s decentralized database. New security concerns raised by BT include common attacks and double-spending. To address the above-mentioned challenges, data analytics on a blockchain-based IoT network is necessary to protect data. The value of emerging technology Machine Learning (ML) is highlighted through analytics on this data. When ML and BT are combined, very precise results may be obtained. Chapter “[An Efficient Blockchain-Based IoT System Using Improved KNN Machine Learning Classifier](#)” is therefore aimed to give a comprehensive study on the use of machine learning to make blockchain-based IoT network smart applications that are more robust to handle network attacks. To investigate these attacks on a

blockchain-based IoT network, an improved K-Nearest Neighbor (KNN) classifier is postulated. It is observed that the Improved KNN (I-KNN) surpasses the Traditional KNN (T-KNN) with an accuracy of 96.7% and 81.6% for the I-KNN classifier and T-KNN, respectively.

Banking sector contributes to 70 % of Indian Gross Domestic Product (GDP) and for India to meet its economic aspirations, it should enable this vivacious sector to grow at 8–10 times of its current pace, in the next 10 years. This pace of active growth requires a double engine of sophisticated technology and a tech-enabled, scalable, and a secured banking system. Implementing Blockchain Technology (BCT) in the banking sector provides a realistic solution which when coupled with devices connected by Internet of Things (IoT) will result in secured, fast-paced, cost-effective, and transparent growth of the sector. The prevalence of personalized banking, secured banking, connected banking, and digital banking are use cases, made possible through interface with IoT. Chapter “[Leveraging Blockchain Technology for Internet of Things Powered Banking Sector](#)” delves into the opportunities in the banking sector to be explored and challenges to be met in the BCT-IoT implementation process. BCT- and IoT-based opportunities such as peer-to-peer lending, Know Your Customer (KYC) updation, cross-border transfer payments, syndicate lending, and fraud reduction are some of the banking operations that are elaborated. To strengthen the banking network, the consensus algorithm of blockchain network is much required and the use of IoT devices to act as nodes is pertinent. The blend of both in the banking space has to be further reinforced.

Internet of Things (IoT) is characterized by heterogeneity of devices, software, and communication protocols when it comes to the implementation of any practical solutions. Especially in use cases such as smart cities, where scalability is very important and increased, the complexity of an Internet of Things system introduces issues on the management and privacy of both (smart) devices and users. Identity and Access Management is the set of policies applied on a system restricting or allowing access of acting entities (devices and users) to the system’s services. OAuth and Single-Sign On are two of the widest used implementations for Identity and Access Management. Chapter “[Identity Management in Internet of Things with Blockchain](#)” targets on exploring the new ways in which blockchain technology can significantly improve Identity Management in IoT by utilizing decentralized identity structures and specific cryptographic techniques applied by it.

Internet of Things is transforming devices making them “smart”, thereby overlapping the digital and physical worlds. Interaction between IoT devices creates networks with unprecedented scalability which however creates many exploitable vulnerabilities due to the lack of built-in security in IoT devices. Blockchain can resolve this particular limitation due to its immutable, decentralized nature. Industrial Internet of Things (IIoT) uses IoT devices to analyze and manage industrial data in real time for various purposes. Thus, protecting this data from different types of attacks is necessary, for which blockchain is viable. In chapter “[An Efficient Hash-Selection-Based Blockchain Architecture for Industrial IoT \(IIoT\)](#)”, the authors have proposed a novel blockchain-based model that groups IIoT devices into tier-based clusters depending on computational capability by benchmarking. Each

cluster is individually more efficient in terms of both energy utilization and security for IIoT systems by using different computationally suitable hash algorithms. The higher efficiency of the proposed model compared to current solutions is proven by experimental results.

A digital ledger which is based on distributed technology will help to address cybersecurity and secrecy problems in the Internet of Things Architecture, but combining these two technologies poses some difficulties. In order to preserve a tradition of financial transactions, cryptocurrencies introduced DL technology. The DL size in a cryptocurrency addresses hundreds of GBs, while the storage of IoT nodes is limited. Similarly, cryptocurrencies implement costly processes of consensus, while IoT nodes in calculation and energy are restricted. Moreover, classic distributed ledger technology (Bitcoin) is not based on quantum. Chapter “[Quantum Aware Distributed Ledger Technology for Blockchain-Based IoT Network](#)” aims on a distributed ledger security based on quantum technology, specifically Distributed Ledger for Internet of Things, for IoT architectures. One cornerstone of the chapter is a new signature creation scheme which is named as Single Time Signature based on time (STS), Blockchain-STS, a compact scheme. Compared with the famous Winternitz-OTS+ system, Blockchain-STS offers a 75 percent reduction in signature size and a 76 percent reduction in signature generation time.

Chapter “[BCoT: Concluding Remarks](#)” summarizes the findings reported in the volume with future directions of research.

The book is intended for researchers, academicians, and practitioners working in the field of blockchain-based IoT. This volume will serve as a readymade material for the researchers and academicians as it covers a wide range of subject areas belonging to several majors falling under the umbrella of blockchain-based Internet of Things for Industry 5.0. The editors will feel rewarded if this edited volume comes to the benefit of the end users.

Kolkata, India
Birbhum, India
Fortaleza-CE, Brazil
February 2022

Debashis De
Siddhartha Bhattacharyya
Joel J. P. C. Rodrigues

Contents

BCoT: Introduction to Blockchain-Based Internet of Things for Industry 5.0	1
Debashis De, Amiya Karmakar, Partha Sarathi Banerjee, Siddhartha Bhattacharyya, and Joel J. P. C. Rodrigues	
Blockchain-Based Internet of Things: Challenges and Opportunities	23
Tripti Paul and Sandip Rakshit	
Challenges and Issues in Blockchain-Based IoT Services	47
Arunima Sharma and Ramesh Babu Battula	
Blockchain for IoT-Based Cyber-Physical Systems (CPS): Applications and Challenges	81
Reham Abdelrazek Ali, Elmoustafa Sayed Ali, Rania A. Mokhtar, and Rashid A. Saeed	
Blockchain in IoT and Beyond: Case Studies on Interoperability and Privacy	113
Abhik Banerjee, Bhaskar Dutta, Tamoghna Mandal, Rajdeep Chakraborty, and Rituparna Mondal	
Hybrid Blockchain-Enabled Security in Cloud Storage Infrastructure Using ECC and AES Algorithms	139
Mhamad Bakro, Sukant K. Bisoy, Ashok K. Patel, and M. Adib Naal	
An Efficient Blockchain-Based IoT System Using Improved KNN Machine Learning Classifier	171
Roseline Oluwaseun Ogundokun, Micheal Olaolu Arowolo, Sanjay Misra, and Robertas Damasevicius	

Leveraging Blockchain Technology for Internet of Things Powered Banking Sector	181
Nayak Surekha, Rangasamy Sangeetha, Chellasamy Aarthy, Rajamohan Kavitha, and R Anuradha	
Identity Management in Internet of Things with Blockchain	209
Maria Polychronaki, Dimitrios G. Kogias, and Charalampos Z. Patrikakis	
An Efficient Hash-Selection-Based Blockchain Architecture for Industrial IoT (IIoT)	237
Susmit Das, Sreyashi Karmakar, and Himadri Nath Saha	
Quantum Aware Distributed Ledger Technology for Blockchain-Based IoT Network	267
Koustav Kumar Mondal and Deepsuhra Guha Roy	
BCoT: Concluding Remarks	289
Siddhartha Bhattacharyya, Partha Sarathi Banerjee, Amiya Karmakar, Debashis De, and Joel J. P. C. Rodrigues	
Index	295

Editors and Contributors

About the Editors

Debashis De is Professor, Department of Computer Science and Engineering & Director of School of Computational Science of MAKAUT, WB, India. He is Senior Member-IEEE, Fellow IETE, Life member CSI. He was awarded the prestigious Boycast Fellowship by the Department of Science and Technology, Government of India, to work at the Heriot-Watt University, Scotland, UK. He received the Endeavour Fellowship Award from 2008 by DEST Australia to work at the University of Western Australia. He received the Young Scientist award both in 2005 at New Delhi and in 2011 in Istanbul, Turkey, from the International Union of Radio Science, Belgium. In 2016 he received the JC Bose research award by IETE, New Delhi. He established the Center of Mobile cloud computing (CMCC) for IoT applications. He is Vice-chair of Dew Computing STC of IEEE Computer Society. He published in 320 journals and 200 conference papers, Fifteen books, and filed ten patents. His h index is 32, citation 5200. Listed in Top 2% Scientist List of the world by Stanford University, USA. His research interest includes Mobile Edge Computing, IoT, and Quantum Computing.

Prof. Siddhartha Bhattacharyya did his Bachelors in Physics, Bachelors in Optics and Optoelectronics and Masters in Optics and Optoelectronics from University of Calcutta, India in 1995, 1998 and 2000 respectively. He completed PhD in Computer Science and Engineering from Jadavpur University, India in 2008. He is the recipient of the University Gold Medal from the University of Calcutta for his Masters. He is the recipient of several coveted awards including the Distinguished HoD Award and Distinguished Professor Award conferred by Computer Society of India, Mumbai Chapter, India in 2017, the Honorary Doctorate Award (D. Litt.) from The University of South America and the South East Asian Regional Computing Confederation (SEARCC) International Digital Award ICT Educator of the Year in 2017. He has been appointed as the ACM Distinguished Speaker for the tenure 2018-2020. He is currently serving as a Professor in the Department of Computer Science and

Engineering of Christ University, Bangalore. He served as the Principal of RCC Institute of Information Technology, Kolkata, India during 2017-2019. He is a co-author of 6 books and the co-editor of 77 books and has more than 300 research publications in international journals and conference proceedings to his credit. His research interests include hybrid intelligence, pattern recognition, multimedia data processing, social networks and quantum computing.

Joel J. P. C. Rodrigues [Fellow, IEEE & AAIA] is a Professor of Senac Faculty of Ceará, Brazil, head of research, development, and innovation; China National Talent at the China University of Petroleum (East China), Qingdao, and senior researcher at the Instituto de Telecomunicações, Portugal. Prof. Rodrigues is an Highly Cited Researcher, the leader of the Next Generation Networks and Applications (NetGNA) research group (CNPq), an IEEE Distinguished Lecturer, Member Representative of the IEEE Communications Society on the IEEE Biometrics Council, and the President of the scientific council at ParkUrbis – Covilhã Science and Technology Park. He was Director for Conference Development - IEEE ComSoc Board of Governors, Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, a Past-Chair of the IEEE ComSoc Technical Committee (TC) on eHealth and the TC on Communications Software, a Steering Committee member of the IEEE Life Sciences Technical Community and Publications co-Chair. He is the editor-in-chief of the International Journal of E-Health and Medical Communications and editorial board member of several high-reputed journals (mainly, from IEEE). He has been general chair and TPC Chair of many international conferences, including IEEE ICC, IEEE GLOBECOM, IEEE HEALTHCOM, and IEEE LatinCom. He has authored or coauthored about 1000 papers in refereed international journals and conferences, 3 books, 2 patents, and 1 ITU-T Recommendation. He had been awarded several Outstanding Leadership and Outstanding Service Awards by IEEE Communications Society and several best papers awards. Prof. Rodrigues is a member of the Internet Society, a senior member ACM, and Fellow of AAIA and IEEE.

Contributors

Chellasamy Aathy School of Business and Management, CHRIST University, Bangalore, India

Elmustafa Sayed Ali Department of Electronics Engineering, Sudan University of Science and Technology, Khartoum, Sudan;
Department of Electrical and Electronics Engineering, Red Sea University, Port Sudan, Sudan

Reham Abdelrazek Ali Department of Electronics Engineering, Sudan University of Science and Technology, Khartoum, Sudan

R Anuradha School of Business and Management, CHRIST University, Bangalore, India

Micheal Olaolu Arowolo Department of Computer Science, Landmark University Omu Aran, Omu-Aran, Nigeria

Ramesh Babu Battula Malviya National Institute of Technology, Jaipur, India

Mhamad Bakro Department Computer Science and Engineering, C. V. Raman Global University, Bhubaneswar, India

Abhik Banerjee Department of Computer Science and Engineering, Netaji Subhash Engineering College, Kolkata, India

Partha Sarathi Banerjee Department of Information Technology, Kalyani Government Engineering College, Kalyani, West Bengal, India

Siddhartha Bhattacharyya Rajnagar Mahavidyalaya, Birbhum, West Bengal, India

Sukant K. Bisoy Department Computer Science and Engineering, C. V. Raman Global University, Bhubaneswar, India

Rajdeep Chakraborty Department of Computer Science and Engineering, Netaji Subhash Engineering College, Kolkata, India

Robertas Damasevicius Department of Software Engineering, Kaunas University of Technology, Kaunas, Lithuania

Susmit Das RCC Institute of Information Technology, Kolkata, India

Debashis De Department Computer Science and Engineering, Centre of Mobile Cloud Computing, Maulana Abul Kalam Azad University of Technology, Kolkata, WestBengal, India

Bhaskar Dutta Department of Computer Science and Engineering, University of Calcutta, Kolkata, India

Deepsubhra Guha Roy Mobile and Cloud Lab, Institute of Computer Science, University of Tartu, Tartu, Estonia

Amiya Karmakar Department Computer Science and Engineering, Centre of Mobile Cloud Computing, Maulana Abul Kalam Azad University of Technology, Kolkata, West Bengal, India

Sreyashi Karmakar RCC Institute of Information Technology, Kolkata, India

Rajamohan Kavitha School of Sciences, CHRIST University, Bangalore, India

Dimitrios G. Kogias Department of Electrical and Electronics Engineering, University of West Attica, Attica, Greece

Tamoghna Mandal Department of Computer Science and Engineering, National Institute of Technology (NIT) Durgapur, Durgapur, West Bengal, India

Sanjay Misra Department of Electrical and Information Engineering, Covenant University to Department of Computer Science and Communication, Ostfold University College, Halden, Norway

Rania A. Mokhtar Department of Electronics Engineering, Sudan University of Science and Technology, Khartoum, Sudan;
Department of Computer Engineering, Taif University, Al-Taif, Kingdom of Saudi Arabia

Koustav Kumar Mondal School of Computational Science, Department of IT, Maulana Abul Kalam Azad University of Technology, Simhat, Haringhata, Nadia, Kolkata, West Bengal, India

Rituparna Mondal Department of Computer Applications, Narula Institute of Technology, Kolkata, India

M. Adib Naal Department Computer Science and Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar, India

Roseline Oluwaseun Ogundokun Department of Computer Science, Landmark University Omu Aran, Omu-Aran, Nigeria

Ashok K. Patel Department Computer Science and Engineering, C. V. Raman Global University, Bhubaneswar, India

Charalampos Z. Patrikakis Department of Electrical and Electronics Engineering, University of West Attica, Attica, Greece

Tripti Paul Indian Institute of Technology (Indian School of Mines), Dhanbad, India

Maria Polychronaki Department of Electrical and Electronics Engineering, University of West Attica, Attica, Greece

Sandip Rakshit American University of Nigeria, Yola, Nigeria

Joel J. P. C. Rodrigues China University of Petroleum (East China), Qingdao, China;
Senac Faculty of Ceará, Fortaleza-CE, Brazil;
Instituto de Telecomunicações, Covilhã, Portugal

Rashid A. Saeed Department of Electronics Engineering, Sudan University of Science and Technology, Khartoum, Sudan;
Department of Computer Engineering, Taif University, Al-Taif, Kingdom of Saudi Arabia

Himadri Nath Saha Surendranath Evening College, Calcutta University, Kolkata, India

Rangasamy Sangeetha School of Business and Management, CHRIST University, Bangalore, India

Arunima Sharma Malviya National Institute of Technology, Jaipur, India

Nayak Surekha School of Business and Management, CHRIST University, Bangalore, India

BCoT: Introduction to Blockchain-Based Internet of Things for Industry 5.0



**Debashis De, Amiya Karmakar, Partha Sarathi Banerjee,
Siddhartha Bhattacharyya, and Joel J. P. C. Rodrigues**

Abstract The Internet of Things is reforming Industry 5.0 to feature blockchain-driven secure connectivity—fundamental characteristics of IoT encounter challenges like decentralization, security vulnerabilities, and deprived interoperability. Blockchain-based centralized technology addresses the challenges of IoT. Blockchain of Things(BCoT) shows the convergence of Blockchain and IoT. The developments in multi-virtual sensor IoT, and heterogeneous multi-system information fusion for BCoT are analyzed in detail. The future challenges of industrial applications of BCoT are discussed in detail. BCoT-based Sustainable Cities and Society (SCS) focuses on developing environmentally, economically, and socially sustainable resilient cities. Dew computing-based BCoT enables the smart city seamless even at unstable Internet connectivity in remote areas.

Keywords Blockchain · Internet of things · BCoT · Smart contract · Decentralized IoT · Scalable IoT · Fog computing · Edge computing · Dew computing

D. De (✉) · A. Karmakar

Department Computer Science and Engineering, Centre of Mobile Cloud Computing, Maulana Abul Kalam Azad University of Technology, Kolkata, WestBengal, India
e-mail: dr.debashis.de@gmail.com

P. S. Banerjee

Department of Information Technology, Kalyani Govt Engg College, Kalyani, West Bengal, India

S. Bhattacharyya
Rajnagar Mahavidyalaya, Birbhum, West Bengal, India

J. J. P. C. Rodrigues

College of Computer Science and Technology, China University of Petroleum (East China),
Qingdao 266555, China

Senac Faculty of Ceará, Fortaleza-CE, Brazil

Covilhã Delegation, Instituto de Telecomunicações, Covilhã, Portugal

1 Introduction

This chapter introduces the integration of blockchain technology with the Internet of Things to connect everything globally. Industry 5.0 is a new dawn in massive automated production based on the active collaboration between the creative potential of people and accurate apparatuses. Internet of Things (IoT) can make environments smarter, increasingly connected, and more profitable and efficient by connecting many distributed and ubiquitously available intelligent devices and sensors through multi-level communication infrastructures. While this should ideally map to a decentralized hardware and software platform, current solutions are mostly based on centralized infrastructures, with many disadvantages, e.g., high maintenance costs, low interoperability, single point of failure, etc. An additional challenge in supporting decentralization is achieving distributed consensus among autonomous IoT objects [1–3]. In this view, blockchain represents a promising solution for enabling a decentralized IoT framework [4–8]. However, due to the heterogeneity, IoT requires addressing several additional challenges, including ensuring scalability, interoperability, security, privacy, and efficiency [9].

Soft computing techniques are applied to analyze and classify data or predict data from various systems—a blockchain shaped as digital transactions occurring among the participants [10–14]. Blockchain is a peer-to-peer network where all participating peers maintain identical copies of the distributed ledger. At the same time, new entries containing information about transactions added to the blockchain utilizing decentralized consensus among the peers. A blockchain is the amalgamation of cryptography, critical public infrastructure, and economic modeling applied to peer-to-peer networking and decentralized consensus to achieve distributed database synchronization from a technological perspective. Besides its ability to digitize transactions smoothly and efficiently, blockchain technology has gone mainstream in various industries such as finance, insurance, logistics, and agriculture [14–18]. Its unique capability is to provide “trustless” networks without centralized authorities so data transacting nodes can reach faster reconciliation [19–23]. As a result, it enables the flourishing of novel decentralized and fully autonomous applications [24–29]. Such applications carry new opportunities, but they also introduce significant challenges for traditional soft computing tools and methodologies that need to be adapted consequently. For example, the machine learning community is leveraging cryptographic techniques such as Multi-Party Computation and Homomorphic Encryption for privacy-preserving training. Blockchain-based distributed intelligent IoT applications.

1.1 *Objectives*

The objective of the work is to.

- (i) deliver an overview of blockchain in the IoT domain;
- (ii) extant in-depth analysis on advantages and applications of blockchain in the Internet of things; and
- (iii) giving discerning deliberations of technical challenges and limitations of blockchain of things.

1.2 *Contributions*

The major contributions of this paper are as follows:

- (1) A transitory introduction on IoT and blockchain is initially given and then the summary of key features of IoT and blockchain is designated.
- (2) A synopsis of key blockchain technologies and IoT is given with its enactment in the Internet of things.
- (3) The main part of this paper is engrossed in blockchain and IoT. In this work, various architectures of the blockchain of things and its applications are demonstrated.
- (4) Furthermore, this work reviews the applications, challenges, and restraint of blockchain of things.

1.3 *Organization of the Paper*

The rest of the chapter is organized as follows. Section 2 examines the background of blockchain technology. Section 3 presents the Internet of things overview. Section 4 describes challenges in IoT, and Sect. 5 examines the basic architecture of blockchain for IoT. In Sect. 6, tools and techniques for blockchain of things are presented. Section 7 talks about the challenges of the blockchain of things and Sect. 8 described the conclusion of the work.

2 Background on Blockchain Technology

Blockchain is a particular type of distributed database. It contains all the data in encrypted form to make a chronological order of a single source of truth for data. The evolution of blockchain and the smart contract also came into the picture [30–34]. A smart contract is a computer code that automates some business logic and runs on the blockchain network. All blockchain data are distributed in the peer-to-peer network [35–38]. Blockchain comes under the hierarchy of Distributed Ledger

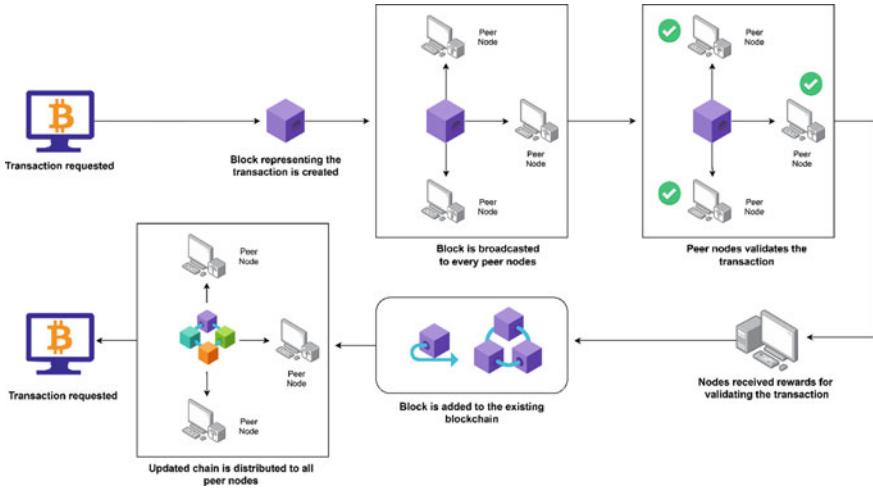


Fig. 1 Block creation in the blockchain network

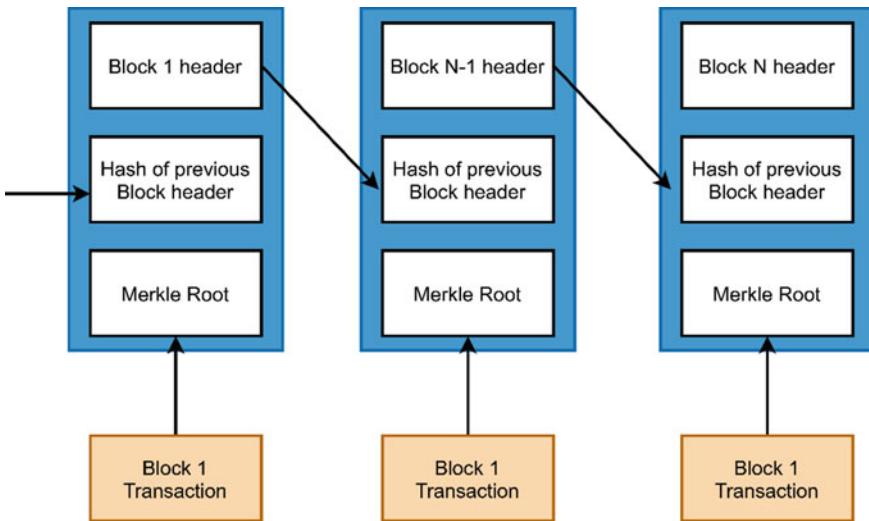
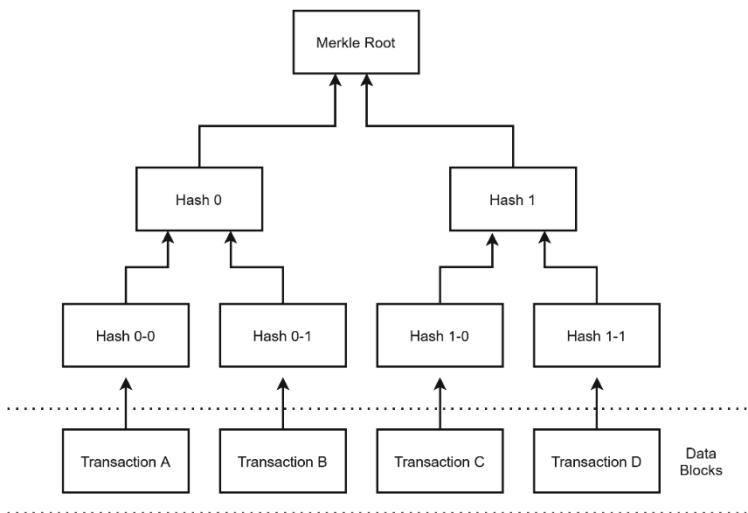
technologies. The main function of this Distributed Ledger technology is creating an immutable chain of blocks linked to the previous root genesis block that contains all the transactions which happened till now, as shown in Fig. 1. The copy of the transactions is broadcasted on all of the nodes that participate in the decentralized network [39–42]. Each transaction performed in the block before it is added to the network is validated through a consensus algorithm.

2.1 Link List Structured Block

In blockchain architecture, every block contains the previous block's hash, as shown in Fig. 2. Therefore, any falsification in the last block is reflected throughout the chain, and all blocks after the tempered block will be invalid.

2.2 Merkle Tree Structure

In blockchain technology, the Merkle tree structure is maintained, as shown in Fig. 3. Every block contains Merkle tree's root hash in this architecture, made with all transaction hashes. Each Merkle tree node is created with concatenated values from its two children. Any falsification in any node reflected on the above layer and the root hash will also be affected. As a result, falsification is detected quickly.

**Fig. 2** Link list structured block**Fig. 3** Merkle tree structure

3 Internet of Things Overview

The world has witnessed unprecedented growth in the number of connected digital devices in recent years. Operating platforms for these digital devices are built up with state-of-the-art sophisticated components which make them work with high precision. The symbiosis of these devices is popularly known as the Internet of

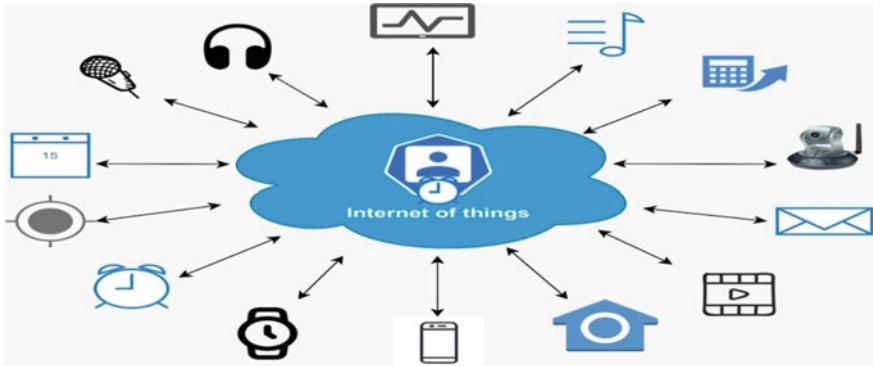


Fig. 4 Integration multiple service framework in IoT

things (IoT) [43–46]. Recent advances in IoT have resulted in a paradigm shift from a computer-aided society to a service-based intelligent organization.

An enormous amount of data needs to be managed to make the IoT-based system work with end-to-end reliability. Cloud-based architectures provide the virtual infrastructure for utility-based computing that integrates monitoring devices, analytics tools, visualization systems. IoT provides a reliable infrastructure for services that require ubiquitous connectivity. Smart connectivity with the existing network architecture and context-based reliable service deployment is the fundamental design challenge for IoT.

The term “Internet of Things” was first coined by Kelvin Ashton in 1999 [47]. In the past few years, the definition has included many applications like healthcare, surveillance, utility, transport, education, etc. [48]. Figure 4 shows a representative diagram of service integration in IoT.

Fueled by the radical evolution of the Internet and the prevalence of devices equipped with wireless technology like Bluetooth, Radio Frequency Identification (RFID), and Wi-Fi, the IoT has transformed the physical world into an intelligent, logical framework with ubiquitous connectivity [49, 50].

Mobile IP-based sensor network builds up the sensing and actuating layer of the infrastructure of IoT. Each sensor node can have an IPv6 address for the unique identification of the device. These sensor nodes detect an event and measure the physical and environmental parameters with high precision so that the IoT-based system can make a correct decision.

3.1 Architecture of IoT

A typical IoT system consists of a layered architecture with the following sub-systems, as shown in Fig. 5. The architecture consists of three sub-layers, viz., sensing and perception layer, communication layer, and application layer.

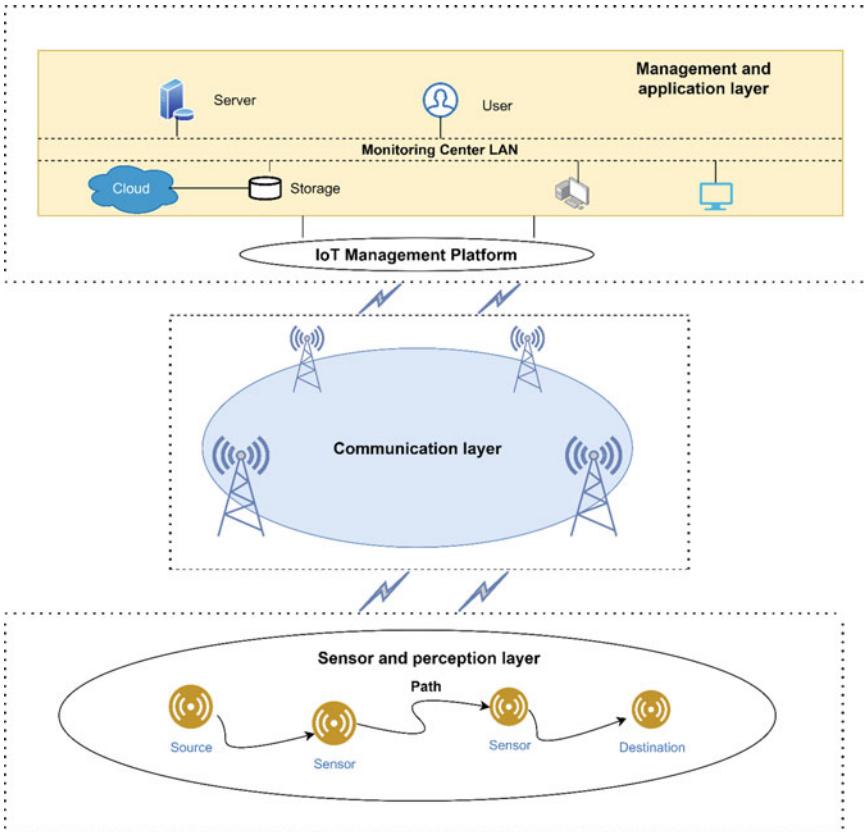


Fig. 5 Illustration of IoT layered architecture

Sensing and perception layer: This layer comprises many IoT devices, including sensors, actuators, controllers, RFID tags, smart meters, and wearable devices. The variety of devices deployed for data acquisitions are collectively called edge devices. These edge devices interface with the environment to collect data. Some specific nodes, equipped with actuators and controllers, classify the data, make decisions, and perform suitable actions according to the environment.

Communication Sub-layer: IoT gateways, Wi-Fi access points, and Base Stations (BS) build up the communication sub-layer of the IoT architecture. The edge devices connect with the nodes in the communication sub-layer by diverse communication protocols like Bluetooth, Near-Field Communication (NFC), Low-power Wireless Personal Area Networks (6LoWPAN), Wireless Highway Addressable Remote Transducer (Wireless HART) [51], and Low-Power Wide Area Networks (LoPWAN) technologies including Sigfox, LoRa, narrowband IoT (NB-IoT), and industrial Ethernet [52]. Different devices are equipped with varying communication technologies, producing a heterogeneous wireless network demanding specialized

middleware and data aggregation protocols [53–58]. IoT is used for a broad spectrum of services strategically integrated to realize a reliable virtual network [59–61]. An efficient middleware combines cyberinfrastructure with Service-Oriented Architecture (SOA) and sensor network to explore the heterogeneous sensor resources [62]. A secure data aggregation is required to implement a reliable and secure data dissemination framework.

Management and Application Sub-layer: Various industrial applications like manufacturing, supply chain, healthcare, surveillance, smart grid, smart home, and online shopping applications were successfully established with IoT-based infrastructure [63–65]. Moreover, efficient use of artificial intelligence and machine learning has launched a user-feedback-based service architecture.

3.2 IoT Integrated Technologies

With the phenomenal progress of IoT, several technologies have been developed or envisioned using intelligent services. We describe some of them in brief in the following.

Fog-IoT Architecture: The recent development of Fog computing is the reliable and ubiquitous service provided by the underlying IoT infrastructure [66–68]. Figure 6 presents a schematic view of the architecture. The Fog computing paradigm utilizes the local computing resources located at the network edge instead of cloud-based data collection and processing. The devices include sensors, actuators, and smart devices that are linked to an IoT platform. Low-latency, real-time precise decision-making, and optimal utilization of available bandwidth are some of the advantages of the combined architecture.

CPS and Dew's architecture based on IoT: Integration of Cyber-Physical Systems (CPS) and Dew computing with IoT efficiently maps the physical devices to secure virtual services [69]. This architecture contains four sub-layers, as shown in Fig. 7. The lowermost layer consists of IoT devices like sensors, actuators, and intelligent wearables, which interact with the physical machines to collect event data. This layer connects to the next level, called the dew layer, which contains smart devices equipped with processing, storage, and communication capability. Then, the upper layer contains edge nodes that interface with the dew layer to extract information from the collected data. This layer is referred to as the Edge device layer. Finally, there is an Edge service layer above this layer that connects the edge devices to the cloud.

Edge-IoT architecture (Edge-of-Things): Integration of Edge computing with IoT brings many advantages for real-time intelligent applications. The cost-effective, energy-efficient, and QoS-aware synergy of the technologies provides an opportunistic data delivery framework that leverages secure and productive infrastructure for the service providers. Figure 8 shows a schematic of the envisioned architecture where intelligent IoT devices and edge devices seamlessly communicate to make the service layer work with expected efficiency.

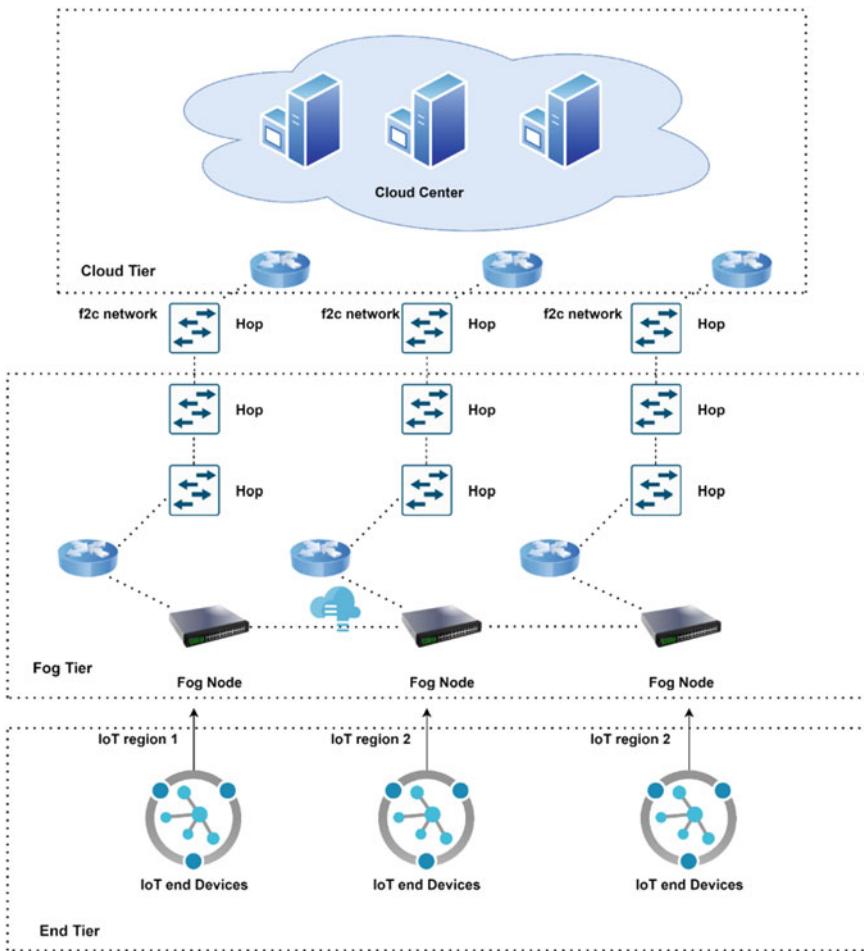


Fig. 6 Illustration of Fog-IoT architecture

4 Challenges in IoT

IoT poses a bunch of research challenges, as mentioned in the following.

Heterogeneity

The interoperability of heterogeneous devices in IoT is a big challenge for researchers. Unified infrastructure for various communication protocols, data types, and hardware architectures is required to build up a successful service framework.

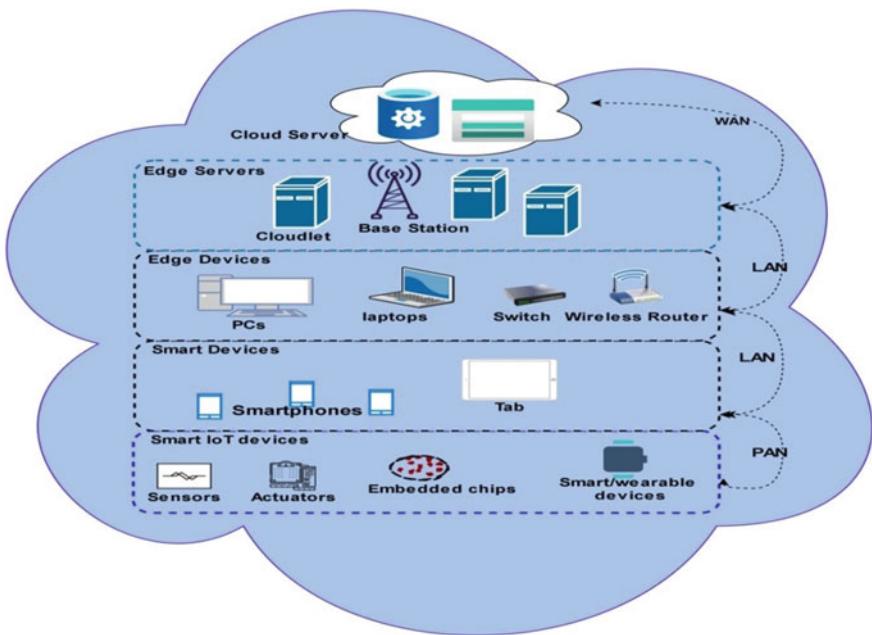


Fig. 7 CPS and Dew architecture based on IoT

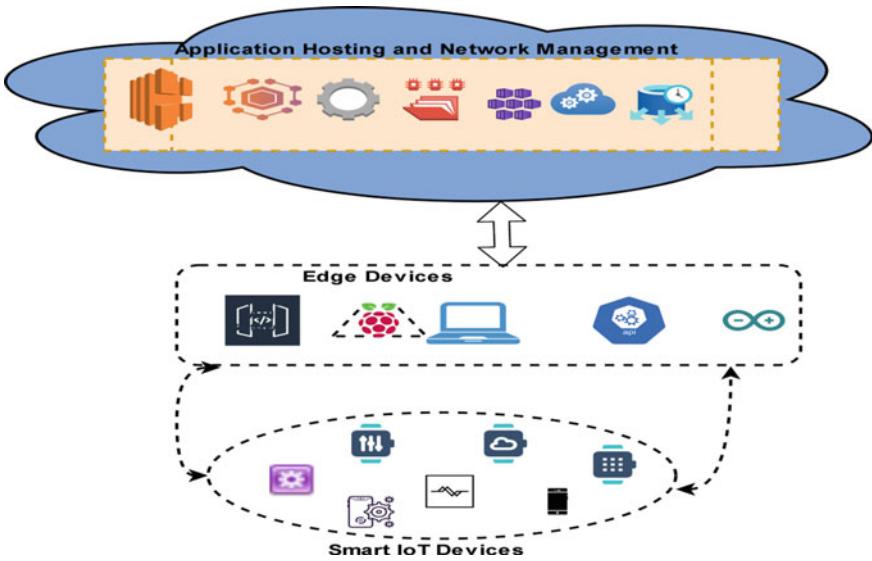


Fig. 8 Illustration of Edge-IoT architecture

Resource constraints

IoT comprises low-power sensor nodes, controllers, actuators, and RFID-based systems. These entities do not carry out computation-intensive execution of algorithms, long-range communication, and high storage of data. Therefore, distributed resource maintenance is a good solution for the proper operation of IoT.

Privacy Vulnerability

Resource constraint nodes, limited interoperability among various technologies, and the requirement of cloud connectivity for centralized storage make the IoT base system vulnerable to security attacks. The peer-to-peer communication architecture of IoT requires distributed security mechanism for a resilient architecture.

The proliferation of intelligent devices with sensing-actuating-communicating capabilities removes the cognizable difference between the physical and virtual worlds. Moreover, real-time interfacing with the environment and AI-based decision-making algorithms makes things act according to the user's need. The introduction of IoT and derived technologies has thus revolutionized the technical aspect of human life.

5 Basic Architecture of Blockchain for IoT

In IoT, data is generated from a physical environment that suffers from noise, sensor drift, trust, integrity, and authentication. Promising technology like blockchain can overcome these limitations of IoT [70–74]. Blockchain enables trust between distributed sensor nodes using cryptographic hash and consensus algorithm. Blockchain also makes the model transparent, immutable, and secure [75–80]. Every node in the blockchain needs to store a copy of the entire blockchain data, and it will keep increasing over time. Most lightweight IoT devices cannot hold and maintain this massive amount of data due to limitations in their architecture[81–84]. So to integrate blockchain in IoT, optimized and efficient architecture is required. In this section, we will cover the possible architecture models of IoT-enabled blockchain.

5.1 *Blockchain in the Gateway of IoT Devices*

In this design, the gateway act as a full node of the blockchain, and every gateway is connected to sensors. It takes data from a different source as a transaction and performs blockchain algorithms [85]. This architecture contains three layers (a) data layer, (b) blockchain layer and c)application layer, as shown in Fig. 9.

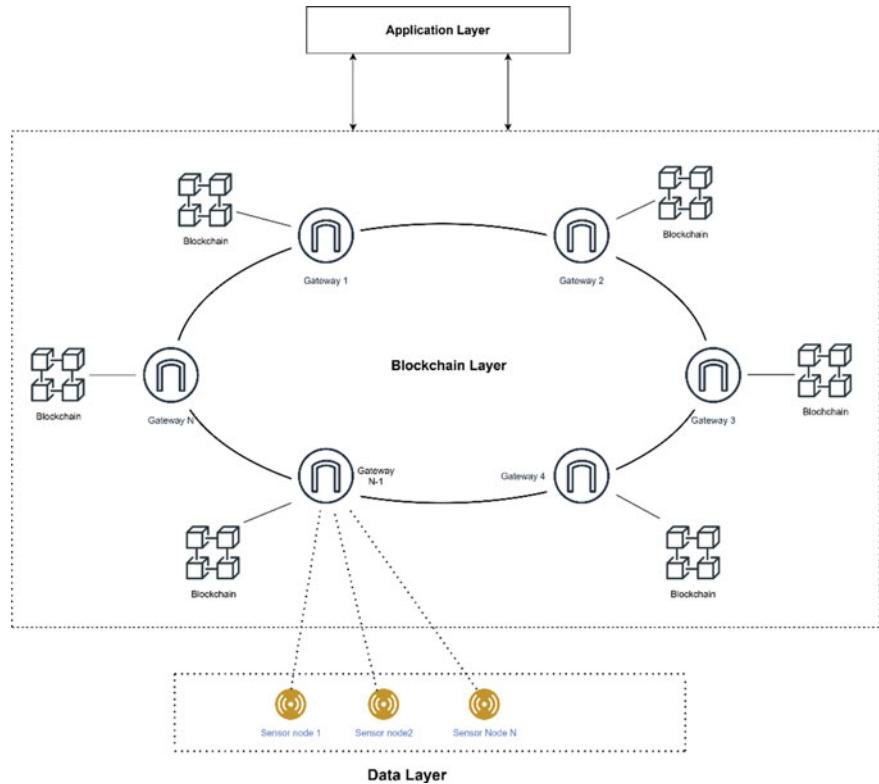


Fig. 9 Blockchain in the gateway of IoT devices architecture

- (a) Data layer: Data layer maintains the collection of data from different IoT sensors and sources. It is responsible for maintaining the physical layer, and it communicates with the blockchain layer to upload the data into the hashed format.
- (b) Blockchain layer: This layer is present in the gateway of IoT, and it maintains all the blockchain principles like blocks generation block validation. It collects the data from the lower tier as transactions and maintains the bridge between the data and application layers.
- (c) Application layer: This layer relays on top of the blockchain layer. It works on data processing and provides interaction between users and service providers.

5.2 Blockchain in Management Hub for IoT

Internet of things is used in several fields like healthcare, finance, agriculture educations, etc. IoT suffers from different security issues, and blockchain can solve this problem [86–91]. But to solve the problem, an optimized architecture is needed.

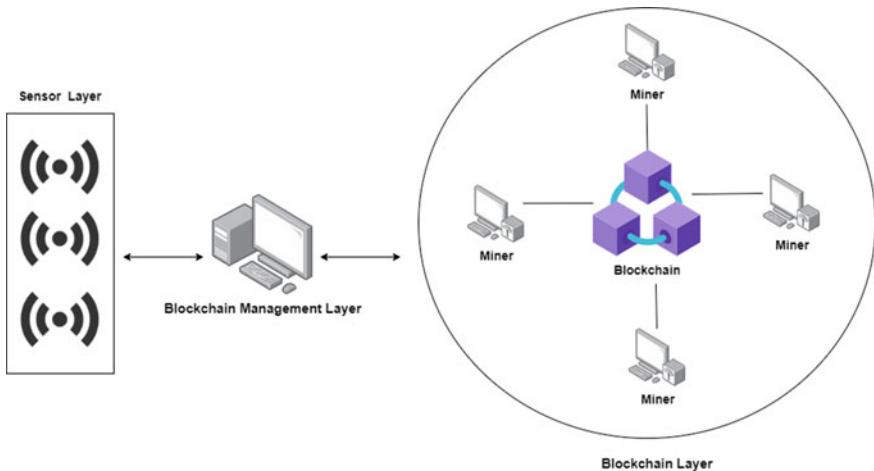


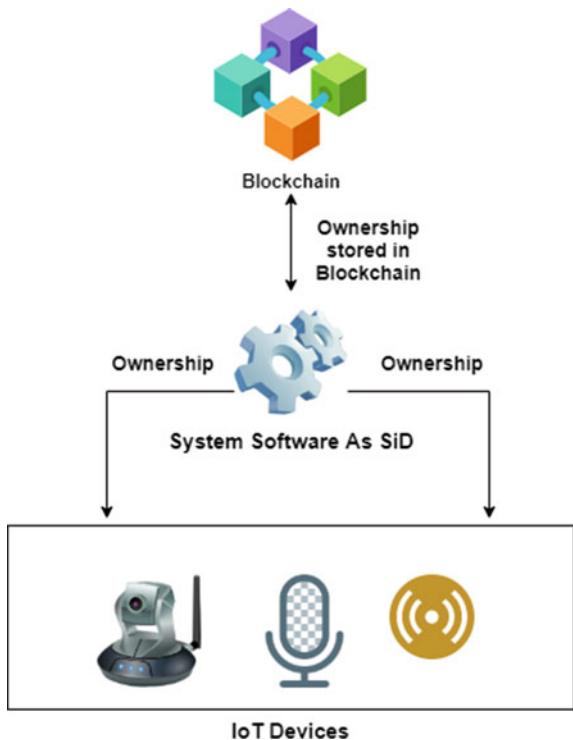
Fig. 10 Management hub-based architecture for blockchain-based IoT

Every blockchain full nodes need to keep all the copies of blockchain data. However, lightweight IoT devices cannot store and maintain this vast amount of data [92–95]. To solve this problem, one dedicated node is integrated with IoT architecture called management hub, as shown in Fig. 10. Management hub contains all the blockchain data, and it interacts with blockchain on behalf of IoT nodes. One smart contract maintains this management hub [96–98]. This contract cannot be deleted and modified. Only the authorized party has control over this smart contract.

5.3 Ownership of IoT Devices Using Dew-Block Architecture

With the power of blockchain, ownership of IoT devices is efficiently controlled in different fields like Fog computing, Dew computing, and cloud computing [99–103]. Software in Dew ensures the software ownership in on-premises devices using Dew computing, and it synchronizes the ownership with the cloud for further use. Cloud can be replaced with blockchain [104, 105]. There is a unique software which is called system software. SiD can control the ownership of any hardware devices using the system software concept. This system software is installed on IoT devices like cameras, vehicles, etc. In this architecture owner of the system, the software is considered the owner of that particular hardware. This system software ownership is synchronized with the blockchain network for further use as shown in Fig. 11.

Fig. 11 Dew-block architecture for IoT device ownership



6 Tools and Techniques for Blockchain of Things

This section described several tools and techniques that are used to develop and interact with the blockchain. Since IoT is used in several things, it needs blockchain tools that simplify developing blockchain [106–108]. Followings are several tools used to create blockchain.

- **Solidity**

Solidity is a high-level statically typed programming language. It is used to implement smart contracts to target Ethereum virtual machines. It also supports inheritance and several libraries.

- **Remix**

The Remix is an open-source browser-based IDE that is used to write smart contracts using solidity language. The Remix helps developers for debugging, testing, and deploying the smart contract into the blockchain network. It is used both locally and is browser based.

- **One-Click Dapp**

“*One click dapp*” is a web-based Distributed app creator that can create Dapp using a simple GUI.

- **Metamask**

Metamask is a wallet that makes a bridge between the browser and Ethereum blockchain. It tracks ether value, allowing users to serve ether whenever they interact with Ethereum Dapps. In addition, Metamask is used directly from the browser.

- **Truffle**

Truffle is a blockchain framework that helps Etherium blockchain developers to develop Ethereum-based decentralized apps. It has a vast library that allows creating a custom deployment for newly written smart contracts.

- **Ganache**

Ganache is an Ethereum blockchain-based tool that helps the user to create a private Ethereum blockchain. Then, users can test their Dapps and execute several commands on that private blockchain.

7 Challenges of Blockchain of Things

Some of the challenges of BCoT in the arena of Industry 5.0 are as follows.

- **Scalability**

In real-time blockchain technology, size of each block is constant, and there is a fixed time interval for creating a new block. In a real-time bitcoin network, nearly seven transactions are processed per second. In a real-time scenario, seven transactions per second are a tiny amount. Since the capacity of each block is tiny and constant as a result, many small transactions are delayed because minors prefer those transactions which contain high transaction fees. So scalability is a huge concern in blockchain technology.

- **Compromise of privacy**

Blockchain is considered a very safe technology for securing privacy. Blockchain cannot guarantee transactional privacy because values regarding all transactions and the user's public keys are visible publicly, disclosing the user's information.

- **Processing power**

A blockchain full node requires enormous processing power to validate a block in the blockchain. Every IoT devices are heterogeneous [109–111], and as a result, processing power is different for every node, and some lightweight node cannot run highweight blockchain algorithms.

- **Storage**

All blockchain nodes need to keep the entire blockchain data in their storage. Here problem comes, maximum IoT device is lightweight and have limited storage. Every IoT device cannot store this massive amount of data. So storage is a considerable concern in the BC-IoT domain.

8 Limitation of Blockchain of Things

Some of the limitations of BCoT in the arena of Industry 5.0 are as follows.

- **Quantum Computing**

Blockchain security is mainly built on some difficult mathematical puzzles which are extremely difficult for conventional computers to crack. However, groundbreaking technology like quantum computing can break this extremely hard mathematical puzzle within few minutes which makes the model vulnerable.

- **51% attack on proof of work**

Proof of work consensus algorithm may suffer from 51% attack, if any node has the majority of computing power that is more than 50%, it can reverse the happened transactions; a node with less than 51% is also dangerous.

- **Selfish mining**

In selfish mining, minors do not reveal the mined blocks into the network; they broadcast the hidden branch once their requirements got satisfied. As a result reviled chain is larger than the current public chain, and all minors admit that longest chain. Before that hidden chain publication, genuine minors wasted their computational power, and selfish minors were mining without competitors and got considerable revenue. If all minor joins in the selfish pool then the system will be vulnerable.

9 Conclusion

IoT has some limitations concerning confidentiality, privacy, and data integrity. Blockchain is one such technology that provides security by design. So blockchain in IoT overcomes the existing limitations of IoT because blockchain provides security, transparency, and availability. However, there are some limitations for a straightforward application of blockchain into IoT, because IoT devices are not capable of running highweight blockchain algorithms and storing huge amounts of data. In this work, we scrutinize the participation of blockchain in IoT. We also provide an inclusive survey on BCoT. In this proposed work, we initially present the Internet of things and blockchain technology. Then, we elaborated on several methods and techniques which enable blockchain into the IoT domain. We further deliberate all the challenges and limitations of BCoT.

Acknowledgements This work is partially funded by FCT/MCTES through national funds and when applicable co-funded EU funds under the Project UIDB/50008/2020; and by Brazilian National Council for Scientific and Technological Development-CNPq, via Grant No. 313036/2020-9.

References

1. Ali MS, Vecchio M, Pincheira M, Dolci K, Antonelli F, Rehmani MH (2018) Applications of blockchains in the internet of things: a comprehensive survey. *IEEE Commun Surv Tutor*, 1–42, 2018. <https://doi.org/10.1109/COMST.2018.2886932>
2. Miraz MH (2020) Blockchain of things (BCoT): the fusion of blockchain and IoT technologies. In: Advanced applications of Blockchain technology, pp 141–159. Springer, Singapore
3. Zhang Y, Wen J (2017) The IoT electric business model: using blockchain technology for the internet of things. *Peer-to-peer networking and applications* 10(4):983–994. <https://doi.org/10.1007/s12083-016-0456-1>
4. Conoscenti M, Vetrò A, De Martin JC (2016) Blockchain for the internet of things: a systematic literature review. In: 2016 IEEE/ACS 13th international conference of computer systems and applications (AICCSA), Nov 2016, pp 1–6
5. Banerjee M, Lee J, Choo K-KR (2018) A blockchain future for internet-of-things security: a position paper. *Digital Commun Netw* 4(3):149–160
6. Reyna A, Martin C, Chen J, Soler E, Daz M (2018) On Blockchain and its integration with IoT. Challenges and opportunities. *Futur Gener Comput Syst* 88:173–190
7. Fernández-Caramés TM, Fraga-Lamas P (2018) A review on the use of blockchain for the internet of things. *IEEE Access* 6:32 979–33 001
8. Deepsubhra Guha R, Das P, De D, Buyya R (2019) QoS-aware secure transaction framework for internet of things using blockchain mechanism. *J Netw Comput Appl* 144:59–78
9. Panarello A, Tapas N, Merlino G, Longo F, Puliafito A (2018) Blockchain and IoT integration: a systematic survey. *Sensors* 18(8). <http://www.mdpi.com/1424-8220/18/8/2575>
10. Sourav H, De D (2020) OBSC: Osmotic BlockChain based framework for Smart City environment. In: 2020 fifth international conference on research in computational intelligence and communication networks (ICRCICN), pp 143–148. IEEE
11. Ray ParthaPratim, Dash D, De D (2019) Internet of things-based real-time model study on e-healthcare: Device, message service, and dew computing. *Comput Netw* 149:226–239
12. Chen M, Miao Y, Hao Y, Hwang K (2017) Narrow band internet of things. *IEEE Access* 5:20557–20577
13. Deepsubhra Guha R, Mahato B, De D, Buyya R (2018) Application-aware end-to-end delay and message loss estimation in the Internet of Things (IoT)—MQTT-SN protocols. *Future Gener Comput Syst* 89(2018):300–316
14. Lu X, Niyato D, Jiang H, Kim DI, Xiao Y, Han Z (April 2018) Ambient backscatter assisted wireless powered communications. *IEEE Wirel Commun* 25(2):170–177
15. Zhou J, Cao Z, Dong X, Vasilakos AV (January 2017) Security and privacy for cloud-based IOT: challenges. *IEEE Commun Mag* 55(1):26–33
16. Roman R, Zhou J, Lopez J (July 2013) On the features and challenges of security and privacy in distributed internet of things. *Comput Netw* 57(10):2266–2279
17. He J, Wei J, Chen K, Tang Z, Zhou Y, Zhang Y (2018) Multitier fog computing with large-scale IoT data analytics for smart cities. *IEEE Int Things J* 5(2):677–686; Zheng Z, Xie S, Dai H-N, Chen X, Wang H (2018) Blockchain challenges and opportunities: a survey. *Int J Web Grid Serv* 14(4): 352–375

18. Deepsubhra Guha R, Mahato B, Ghosh A, De D (2019) Service aware resource management into cloudlets for data offloading towards IoT. *Microsyst Technol*, 1–15
19. Miguel C, Barbara L (1999) Practical Byzantine fault tolerance. In: Proceedings of the third symposium on operating systems design and implementation, vol 99, New Orleans, USA, pp 173–186
20. Li X, Jiang P, Chen T, Luo X, Wen Q (2017) A survey on the security of blockchain systems. *Future Gener Comput Syst*
21. Conti M, SKE, Lal C, Ruj S (2018) A survey on security and privacy issues of bitcoin. *IEEE Commun Surv Tutor*, 1
22. Chase B, MacBrough E (2018) Analysis of the XRP Ledger consensus protocol. arXiv preprint [arXiv:1802.07242](https://arxiv.org/abs/1802.07242)
23. Gilad Y, Hemo R, Micali S, Vlachos G, Zeldovich N (2017) Algorand: Scaling byzantine agreements for cryptocurrencies. In: Proceedings of the 26th symposium on operating systems principles. ACM, 2017, pp 51–68
24. Yu FR, Liu J, He Y, Si P, Zhang Y (2018) Virtualization for distributed ledger technology (vDLT). *IEEE Access* 6:25019–25028
25. Dinh TTA, Wang J, Chen G, Liu R, Ooi BC, Tan K-L (2017) Blockbench: a framework for analyzing private blockchains. In: Proceedings of the 2017 ACM international conference on management of data, ser. SIGMOD '17. New York, NY, USA: ACM, 2017, pp 1085–1100. <https://doi.org/10.1145/3035918.3064033>
26. Zyskind G, Nathan O, Pentland A (2015) Decentralizing Privacy: Using Blockchain to protect personal data. In: 2015 IEEE security and privacy workshops, May 2015, pp 180–184
27. Chawathe SS (2019) Clustering Blockchain data. Springer International Publishing, Cham, pp 43–72
28. Ream J, Chu Y, Schatsky D (2016) Upgrading blockchains: smart contract use cases in industry. Deloitte Press
29. Szabo N (1997) “The idea of smart contracts,” Nick Szabo’s Papers and Concise Tutorials, 1997. [fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart contracts 2.html](http://fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart%20contracts%20.html)
30. Idelberger F, Governatori G, Riveret R, Sartor G (2016) Evaluation of logic-based smart contracts for blockchain systems. In: International symposium on rules and rule markup languages for the semantic web (RuleML). Springer, pp 167–183
31. Sillaber C, Waltl B (Aug 2017) Life cycle of smart contracts in blockchain ecosystems. *Datenschutz und Datensicherheit DuD* 41(8):497–500
32. Koulu R (2016) Blockchains and online dispute resolution: smart contracts as an alternative to enforcement. *SCRIPTed* 13:40
33. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>
34. “Ethereum: Blockchain APP Platforms”. www.ethereum.org/
35. “GMOs: the blockchain operating system. <https://enterprise.gem.co/> [37]; MultiChain: Open platform for building blockchains. <https://www.multichain.com/>
36. Roy S, Sarkar D, Hati S, De D (2018) Internet of music things: an edge computing paradigm for opportunistic crowdsensing. *J Supercomput* 74(11):6069–6101
37. Hyperledger project (2015) <https://www.hyperledger.org/>
38. Xu X, Weber I, Staples M, Zhu L, Bosch J, Bass L, Pautasso C, Rimba P (2017) A taxonomy of blockchain-based systems for architecture design. In: IEEE international conference on software architecture (ICSA), pp 243–252
39. Consortium chain development. <https://github.com/ethereum/wiki/wiki/Consortium-Chain-Development>
40. Johnson D, Menezes A, Vanstone S (2001) The elliptic curve digital signature algorithm (ECDSA). *Int J Inf Secur* 1(1):36–63
41. Christidis K, Devetsikiotis M (2016) Blockchains and smart contracts for the internet of things. *IEEE Access* 4:2292–2303

42. Lu Q, Xu X (2017) Adaptable blockchain-based systems: a case study for product traceability. *IEEE Softw* 34(6):21–27
43. Zhang Y, Wen J (2015) An IoT electric business model based on the protocol of bitcoin. In: Proceedings of 18th international conference on intelligence in next generation networks (ICIN), pp 184–191
44. He S, Xing C, Zhang L-J (2018) A business-oriented schema for blockchain network operation. In: Chen S, Wang H, Zhang L-J (eds) *Blockchain—ICBC 2018*. Springer International Publishing, Cham, pp 277–284
45. Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. *Comput Netw* 54(15):2787–2805
46. Jayawardhana G, Buyya R, Marusic S, Palaniswami M (2013) Internet of things (IoT): a vision, architectural elements, and future directions.“ Future generation computer systems 29(7):1645–1660
47. Kevin A (2009) That ‘internet of things’ thing. *RFID J* 22(7):97–114
48. Sundmaeker H, Guillemin P, Friess P, Woelfflé S (2010) Vision and challenges for realizing the internet of things, cluster of european research projects on the internet of things—CERP IoT
49. Buckley J (ed) (2006) *The internet of things: from RFID to the next-generation pervasive networked systems*. Auerbach Publications, New York
50. Dai H-N, Zheng Z, Zhang Y (2019) Blockchain for Internet of things: a survey. *IEEE Int Things J* 6(5):8076–8094
51. Petersen S, Carlsen S (Dec 2011) WirelessHART versus ISA100.11a: the format war hits the factory floor. *IEEE Ind Electron Mag* 5(4):23–34
52. Mekki K, Bajic E, Chaxel F, Meyer F (2018) A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express*
53. Bera S, Misra S, Vasilakos AV (Dec 2017) Software-defined networking for the internet of things: a survey. *IEEE Int Things J* 4(6):1994–2008
54. Kalkan K, Zeadally S (September 2018) Securing internet of things with software-defined networking. *IEEE Commun Mag* 56(9):186–192
55. Sharma PK, Singh S, Jeong Y, Park JH (2017) Distblocknet: a distributed blockchain-based secure sdn architecture for IoT networks. *IEEE Commun Mag* 55(9):78–85
56. Alvarenga ID, Rebello GAF, Duarte OCMB (2018) Securing configuration management and migration of virtual network functions using blockchain. In: NOMS 2018–2018 IEEE/IFIP network operations and management symposium, April 2018, pp 1–9
57. Afolabi I, Taleb T, Samdanis K, Ksentini A, Flinck H (2018) Network slicing and Softwarization: a survey on principles, enabling technologies, and solutions. *IEEE Commun Surv Tutor* 20(3):2429–2453
58. Ghosh A, Das SK (2008) Coverage and connectivity issues in wireless sensor networks: a survey. *Pervasive Mob Comput* 4:303–334
59. Ortega V, Bouchmal F, Monserrat JF (June 2018) Trusted 5g vehicular networks: Blockchains and content-centric networking. *IEEE Veh Technol Mag* 13(2):121–127
60. Fan K, Ren Y, Wang Y, Li H, Yang Y (2018) Blockchain-based efficient privacy-preserving and data sharing scheme of content-centric network in 5g. *IET Commun* 12(5):527–532
61. Chen C, Lin M, Liu C (2018) Edge computing gateway of the industrial internet of things using multiple collaborative microcontrollers. *IEEE Network* 32(1):24–32
62. Banerjee P, Nath Mandal S, De D (2019) Biswajit Maiti. “i Sleep: thermal entropy aware intelligent sleep scheduling algorithm for wireless sensor network. *Microsystem Technol*, 1–19
63. Xiong Z, Zhang Y, Niyato D, Wang P, Han Z (August 2018) When mobile Blockchain meets edge computing. *IEEE Commun Mag* 56(8):33–39
64. Liu M, Yu FR, Teng Y, Leung VCM, Song M (2018) Computation offloading and content caching in wireless blockchain networks with mobile edge computing. *IEEE Trans Veh Technol* 67(11): 11008–11021

65. Banerjee P, Nath Mandal S, De D, Maiti B (2020) RL-sleep: temperature adaptive sleep scheduling using reinforcement learning for sustainable connectivity in wireless sensor networks. *Sustain Comput Inform Syst* 26
66. Yousef A (2019) A fog computing based architecture for IoT services and applications development. arXiv preprint [arXiv:1911.02403](https://arxiv.org/abs/1911.02403)
67. Zhou Z, Liu P, Feng J, Zhang Y, Mumtaz S, Rodriguez J (2019) Computation resource allocation and task assignment optimization in vehicular fog computing: a contract-matching approach. *IEEE Trans Veh Technol*, 1–1 (Early Access). <https://doi.org/10.1109/TVT.2019.2894851>
68. Li L, Guo M, Ma L, Mao H, Guan Q (2019) Online workload allocation via fog-fog-cloud cooperation to reduce IoT task service delay. *Sensors* 19(18):3830
69. Marjan G (2020) Dew computing architecture for cyber-physical systems and IoT. *Internet Things* 11:100186
70. Wan J, Li J, Imran M, Li D, e-Amin F (2019) A blockchain-based solution for enhancing security and privacy in smart factory. *IEEE Trans Industr Inform*, 1–9 (Early Access). <https://doi.org/10.1109/TII.2019.2894573>
71. Konstantinidis I, Siaminos G, Timplalexis C, Zervas P, Peristeras V, Decker S (2018) Blockchain for business applications: a systematic literature review. In: Abramowicz W, Paschke A (eds) *Business Information Systems*. Springer International Publishing, Cham, pp 384–399
72. Kim HM, Laskowski M (2018) Toward an ontology-driven blockchain design for supply-chain provenance. *Intell Syst Accou Finan Manag* 25(1):18–27
73. Tapscott A, Tapscott D (2017) How blockchain is changing finance. *Harv Bus Rev* 1
74. Kshetri N (2018) 1 blockchains roles in meeting key supply chain management objectives. *Int J Inf Manage* 39:80–89
75. Li Z, Guo H, Wang WM, Guan Y, VatankhahBarenji A, Huang GQ, McFall KS, Chen X (2019) A blockchain and automl approach for open and automated customer service. *IEEE Trans Industr Inform*, 1–9
76. Tse D, Zhang B, Yang Y, Cheng C, Mu H (2017) Blockchain application in food supply information security. In: 2017 IEEE international conference on industrial engineering and engineering management (IEEM), Dec 2017, pp 1357–1361
77. Tian F (2016) An agri-food supply chain traceability system for China based on RFID & blockchain technology. In: 13th international conference on service systems and service management (ICSSSM), 2016, pp 1–6
78. Sander F, Semeijn J, Mahr D (2018) The acceptance of blockchain technology in meat traceability and transparency. *British Food J*
79. Bettín-Díaz R, Rojas AE, Mejía-Moncayo C (2018) Methodological approach to the definition of a blockchain system for the food industry supply chain traceability. In: Computational science and its applications—ICCSA 2018. Cham: Springer International Publishing, 2018, p. 19–33
80. Lin Q, Wang H, Pei X, Wang J (2019) Food safety traceability system based on blockchain and epcis. *IEEE Access* 7:20698–20707
81. Ray ParthaPratim, Dash D, De D (2020) Real-time event-driven sensor data analytics at the edge-Internet of Things for smart personal healthcare. *J Supercomput* 76(9):6648–6668
82. Li Z, Kang J, Yu R, Ye D, Deng Q, Zhang Y (Aug 2018) Consortium Blockchain for secure energy trading in industrial internet of things. *IEEE Trans Industr Inf* 14(8):3690–3700
83. Aitzhan NZ, Svetinovic D (Sept 2018) Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Trans Dependable Secure Comput* 15(5):840–852
84. Pop C, Cioara T, Antal M, Anghel I, Salomie I, Bertонcini M (2018) Blockchain-based decentralized management of demand response programs in smart energy grids. *Sensors* 18(1); Wang K, Shao Y, Shu L, Zhu C, Zhang Y (2016) Mobile big data fault-tolerant processing for health networks. *IEEE Netw* 30(1): 36–42

85. Volkan D, Jurdak R, Putra GD, Dorri A, Kanhere SS (2019) A trust architecture for blockchain in IoT. In: Proceedings of the 16th EAI international conference on mobile and ubiquitous systems: computing, networking and services, pp 190–199
86. Novo O (2018) Blockchain meets IoT: an architecture for scalable access management in IoT. *IEEE Internet Things J* 5(2):1184–1195
87. Griggs KN, Osipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T (2018) Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J Med Syst* 42(7):130. <https://doi.org/10.1007/s10916-018-0982-x>
88. Bhuiyan MZA, Zaman A, Wang T, Wang G, Tao H, Hassan MM (2018) Blockchain and big data to transform the healthcare. In: Proceedings of the international conference on data processing and applications, ser. DPA. ACM, 2018, pp 62–68
89. Sun Y, Zhang R, Wang X, Gao K, Liu L (2018) A decentralizing attribute-based signature for healthcare blockchain. In: 2018 27th international conference on computer communication and networks (ICCCN), 2018, pp 1–9
90. Rahman MA, Hossain MS, Loukas G, Hassanain E, Rahman SS, Alhamid MF, Guizani M (2018) Blockchain-based mobile edge computing framework for secure therapy applications. *IEEE Access* 6:72469–72478
91. Yang Z, Yang K, Lei L, Zheng K, Leung VCM (2018) Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet Things J*, 1–10, May 2018 (Early Access). <https://doi.org/10.1109/JIOT.2018.2836144>
92. Liu H, Zhang Y, Yang T (May 2018) Blockchain-enabled security in electric vehicles cloud and edge computing. *IEEE Network* 32(3):78–83
93. Kang J, Yu R, Huang X, Maharjan S, Zhang Y, Hossain E (Dec 2017) Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. *IEEE Trans Industr Inf* 13(6):3154–3164
94. Kang J, Yu R, Huang X, Wu M, Maharjan S, Xie S, Zhang Y (2019) Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Int Things J*, 1–11
95. Anwesha M, De D, Ghosh SK (2020) FogIoHT: a weighted majority game theory-based energy-efficient delay-sensitive fog network for internet of health things. *Internet Things* 11:100181
96. Mukherjee A, Deb P, De D, Buyya R (2019) IoT-F2N: An energy-efficient architectural model for IoT using Femtolet-based fog network. *J Supercomput* 75(11):7125–7146
97. Ray ParthaPratim, Dash D, De D (2019) Edge computing for internet of things: a survey, e-healthcare case study and future direction. *J Netw Comput Appl* 140:1–22
98. Ray ParthaPratim, Dash D, De D (2019) A systematic review and implementation of IoT-based pervasive sensor-enabled tracking system for dementia patients. *J Med Syst* 43(9):1–21
99. ParthaPratim R, Dash D, De D (2019) Analysis and monitoring of IoT-assisted human physiological galvanic skin response factor for smart e-healthcare. *Sensor Rev*
100. Roy S, Sarkar D, De D (2020) Entropy-aware ambient IoT analytics on humanized music information fusion. *J Ambient Intell Humaniz Comput* 11(1):151–171
101. Sayan Kumar R, De D (2020) Genetic algorithm-based internet of precision agricultural things (IoT) for agriculture 4.0. *Internet of Things*, 100201
102. Ahmed N, De D, Hussain I (2018) Internet of Things (IoT) for smart precision agriculture and farming in rural areas. *IEEE Internet Things J* 5(6):4890–4899
103. Aakashjit B, De D (2021) AgriEdge: edge intelligent 5G narrow band internet of drone things for agriculture 4.0. In: IoT-based intelligent modelling for environmental and ecological engineering, pp 49–79. Springer, Cham
104. Anirbit S, Debnath B, Das A, De D (2021) FarmFox: a quad-sensor based IoT box for precision agriculture. *IEEE Consumer Electron Mag*
105. Wang Y, Gusev M (2019) Decentralized hardware ownership control: dew computing with Blockchain. *API* 9:11
106. Mukherjee A, Dey N, De D (2020) EdgeDrone: QoS aware MQTT middleware for mobile edge computing in opportunistic Internet of Drone Things. *Comput Commun* 152:93–108

107. Nurzaman A, De D, Iftekhar Hussain Md (2018) A QoS-aware MAC protocol for IEEE 802.11 ah-based internet of things. In: 2018 fifteenth international conference on wireless and optical communications networks (WOCN), pp 1–5. IEEE
108. ParthaPratim R, Dash D, De D (2020) Intelligent internet of things enabled edge system for smart healthcare. National Acad Sci Lett, 1–6
109. Kaustabh G, Karmakar A, Banerjee PS (2021) ValveCare: a fuzzy based intelligent model for predicting heart diseases using arduino based IoT infrastructure. In: International conference on computational intelligence in communications and business analytics, pp 229–242. Springer, Cham
110. Ray ParthaPratim, Dash D, De D (2019) Approximation of fruit ripening quality index for IoT based assistive e-healthcare. *Microsyst Technol* 25(8):3027–3036
111. ParthaSarathi B, Karmakar A, Dhara M, Ganguly K, Sarkar S (2021) A novel method for predicting bradycardia and atrial fibrillation using fuzzy logic and Arduino supported IoT sensors. *Med Novel Technol Dev* 10:100058

Blockchain-Based Internet of Things: Challenges and Opportunities



Tripti Paul and Sandip Rakshit

Abstract The majority of interaction in an IoT (Internet of Things) ecosystem occurs via Machine-to-Machine interactions. As a result, establishing confidence among the participating equipment is a significant challenge, particularly given the fact that IoT technology has not been adequately addressed. The Blockchain enables autonomous smart devices and completely removes the need for intermediary parties. However, since Blockchain enables increased scalability, security, dependability, and privacy, it can function as a catalyst in this area. This may be accomplished by utilizing Blockchain technology to monitor and utilize billions of devices connected to IoT ecosystems in order to facilitate and/or coordinate transaction processing. By eliminating a single point of failure, the implementation of Blockchain in the IoT ecosystem will also improve reliability. The cryptographic algorithms used to encrypt the block data and the hashing techniques can provide additional security.

Keywords Blockchain · Internet of things · Decentralized ledger · Hybrid blockchain

1 Introduction

The Internet of Things (IoT) is an evolving technology that has evolved and achieved tremendous reach without human–human workers' involvement in science and engineering applications to solve problems [1]. That makes it possible to create an interaction between human to machine, machine to machine, often smart working force. A popular operating picture (COP) was made possible by the IoT through numerous modern-day living applications [6]. The COP is done through the developments seen in wireless sensor network systems that have connected across the network, sharing

T. Paul

Indian Institute of Technology (Indian School of Mines), Dhanbad, India

S. Rakshit (✉)

American University of Nigeria, Yola, Nigeria

e-mail: sandip.rakshit@aun.edu.ng

data and conducting different analyses [9]. Therefore, it is clearly understood that IoT is not a single technology; it is a mixture of different technologies that will work to achieve smartness [25]. These innovations include communication technology, IT, electronic sensor and actuator technology, and developments in computing and analytics that are trending [20]. When operating from a broader and larger application point of view, integrating all such technologies could make it complicated and difficult to manage [2].

Thus, the IoT is characterized as an internet-based network of connected objects for data collection and sharing. Protection, storage, cost and cloud attacks, and privacy concern billions of connected devices in IoT [21]. The storage of large data volumes raises the question of cloud platform storage and security. With ongoing developments in Blockchain, new transformations in the IoT industry will be brought about. Blockchain helps to monitor billions of connected devices, process transactions, and communicate between IoT devices [28]. Blockchain's decentralized solution prevents the failure of a single source, thereby ensuring the IoT industry's most robust framework. Due to the convergence of Blockchain and IoT, IoT industry producers will benefit from significant cost savings [14].

Cryptographic signatures improve the IoT security feature. The tamper-proof data guarantees an immutable and timestamped transaction [9]. The distributed storage of IoT data saves the expense of IoT by avoiding service providers' monopoly and the cost of harm to hackers. Distributed ledger offers smart contract trust between parties and IoT devices, and automated services. While the IoT has many advantages and can solve various problems in different fields, there are still challenges [16]. Such difficulties may be in the form of solving security problems, privacy concerns, etc.

A blockchain is like a distributed ledger that's open to everyone. The technique has an attractive feature that, once any data has been registered in a blockchain, it becomes very difficult to modify [18]. Bitcoin is the first successful blockchain implementation. Bitcoin is cash that is digital. It is a digital currency and online payment mechanism that uses cryptographic methods to monitor the creation of currency units and validate money's movement, functioning independently of a central bank [3].

Today the world has discovered blockchain technology implementations in many sectors, where trust is needed without the intervention of a centralized authority [24]. The blockchain technique was originally established by a team of researchers in 1991 and was originally designed to timestamp digital documents so that they could not be backed up or tampered with, just like a notary; though, it was totally unused before Satoshi Nakamoto adapted it to create the digital Bitcoin cryptocurrency in 2008 [18].

The blockchain network has no central authority. That really is the concept of a democratized structure. The data is available to everyone and anyone to see because it is a distributed and unchangeable ledger [17]. Therefore, whatever is created on the Blockchain is transparent and everyone involved is responsible and accountable [22].

2 Concept of Blockchain Technology

Blockchain is an incorruptible immutable and distributed system. It is just an online distribution system that can store information, and it is based on interconnected blocks [29].

2.1 Structure of a Block

Every block contains the following: (i) some data, (ii) the hash of the block, and (iii) the hash of the previous block (Fig. 1).

Data: The data stored within the block depends on the form of Blockchain. The data is stored cryptographically. For example, the Bitcoin blockchain stores the information of such transactions, such as the source, the recipient, the numbers of coins, and the transaction's timestamp [5].

Hash: Every block has a distinctive hash-code (hash). A block is identified by its hash that is always unique, just as a fingerprint. At the time of the creation of a new block, its unique hash is generated. Therefore, changing something inside a block causes the hash to change. If the hash of a block changes, it is no longer the same block. Thus, hashes are very useful when someone wants to detect the changes of a block [4].

Hash of the previous block: the tired element inside each block is the previous block's hash. That effectively creates a chain of blocks, and it is this technique that makes a blockchain secure [20].

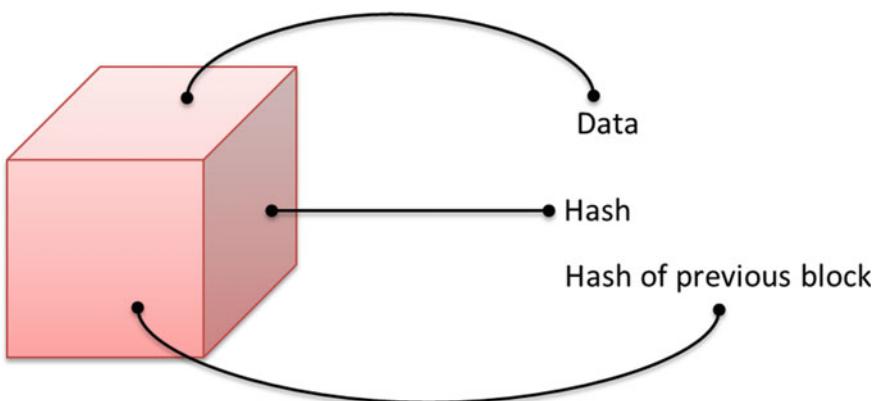


Fig. 1 Structure of a block

2.2 Structure of Blockchain

A blockchain is a timestamped collection of immutable digital records maintained by a cluster of computers not owned by any single individual. Each of these blocks of data is secured and bound to each other using cryptographic principles. Therefore, a blockchain is a chain of blocks that contains information (Fig. 2).

In the above example, the Blockchain has three blocks; each block has a hash and the previous block hash. Thus, block 3 points to block 2, while block 2 points to block 1. The first block is a little unique in that it cannot refer to the preceding block due to the fact that it is the first. Therefore, the first block of a blockchain is called the genesis block [24].

Now let us say that somebody tampers with the second block. That causes the hash of the block to change as well (for example, 7AW2 to H65Y). As a result, block 3 and all subsequent blocks become invalid, as they no longer include a valid hash of the previous block. Thus, altering a single block renders all subsequent blocks invalid [15].

However, using hashes alone is insufficient to avoid manipulation; because computer these days are very fast and can calculate hundreds of thousands of hashes per second. Thus, there is a possibility that someone could successfully tamper with a block and recalculate all the hashes of subsequent blocks to restore the validity of your Blockchain. So to mitigate this, Blockchain has a technique called proof-of-work [26].

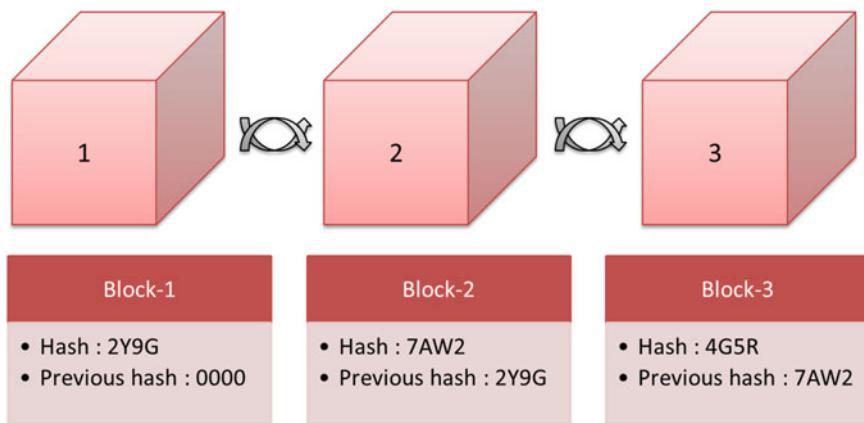


Fig. 2 Example of a blockchain

2.3 Decentralized Ledger

The decentralized ledger is the middle layer in a blockchain architecture that confirms a global ledger that is consistent and temper-proof. Transactions can be grouped in this layer into blocks that are connected cryptographically to each other. A shared and replicated database that is synchronized among the network participants is a decentralized ledger [11]. It keeps the transaction records among the network participants. The ledger has to keep track of transactions among the participants. It stores the information in the header, and data is stored in the form of a token or a cryptocurrency; Blockchain has a database property. Transactions can be described as the exchange of tokens between two parties, and before it is considered a legal transaction, each transaction goes through the validation process [23].

2.4 Proof-of-Work

Proof-of-work is a mechanism that provides security through the prevention of fraud. This security ensures that independent data processors cannot lie about a transaction. Bitcoins calculate the necessary proof-of-work and add a new block to the chain every around ten minutes [5]. Although proof-of-work slows down creating new blocks, this mechanism makes it very difficult to tamper with blocks. Furthermore, if anyone tries to tamper with a block, he/she would need to recalculate the proof-of-work for all the following blocks. So the protection of the Blockchain comes from its innovative use of the hashing and proof-of-work mechanism [4].

2.5 Peer-to-Peer

Peer-to-peer is another technique that blockchains protect themselves, and that is through their distributed nature. Rather than relying on a single institution to administer the chain, blockchains operate via a peer-to-peer network that anyone can join. When a member of this network joins, he or she receives a complete copy of the Blockchain. This may be used by the node to ensure that everything is still in order [17].

If someone creates a new block, then the new block is sent to everyone on the network. All nodes in the block verify to make sure that it has not been tampered with. When everything is verified, each node adds this block to everyone's ledger in the network [5]. New blocks are always added to the Blockchain in a sequential and linear order (Fig. 3).

The consensus is generated by all the nodes (users) in the network. They have reached an agreement on which blocks are valid and which are invalid. Other nodes in the network will reject blocks that are tampered with. So to successfully tamper

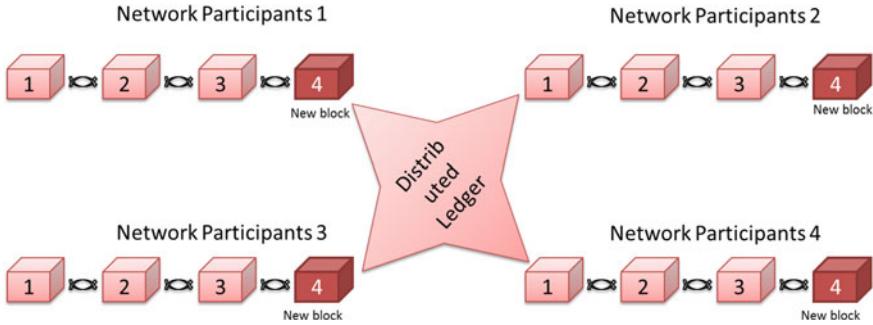


Fig. 3 A new verified block (block-4) is added to everyone's ledger on the network

with a Blockchain, someone will need to tamper with all blocks on the chain, repeat the proof-of-work for each block and take control of more than 50% of the peer-to-peer network. Only then will the tampered block become accepted by everyone else. That is almost impossible to do [15].

2.6 Miners

These databases or ledgers are run by different individuals, often called “miners”, and sometimes “nodes” or “validators”. Some of the nodes may be “partial” (as opposed to full function), of course, and some of the miners may be in a “mining pool” [29].

Users will trust the public ledger system stored globally on multiple different decentralized nodes operated by “miner-accountants” in contrast to establishing and maintaining trust with the transaction counterpart (another person) or a third-party intermediary (like a bank). The main breakthrough is the Blockchain as the architecture for a modern scheme of open, trustless transactions. On a global scale, the Blockchain permits the disintermediation and decentralization of all transactions of some sort between all parties [22].

3 Benefits of Using Blockchain

The Blockchain is an easy but innovative way to move information fully automated and secure from point-A to point-B. Blockchain Technology's key properties that have helped it achieve widespread acclaim are as follows: decentralization, transparency, immutability, and Abstraction [14].

Decentralization: Blockchain technology operates on the idea of a shared database where several machines contain these databases, and each copy of this database is identical. The world had been more used to centralized networks before

Bitcoin and BitTorrent came along. The concept is quite simple. You have a centralized organization that has processed all the information, and you have to deal with this entity alone in order to access whatever information you need. An example of a centralized system is the banks. All of your money is deposited with them, and the only way you can pay anyone is by going through the bank. However, for several years, centralized systems have served us well, but they have many disadvantages. First, since it is centralized, all the information is collected in one location. For potential hackers, this makes them simple target spots. Second, if a software update were to go through the centralized system, it would interrupt the whole system. Third, when, for an unknown reason, the centralized body somehow shuts down. Nobody would then be able to access the data they possess, where the information is not stored by one single entity in a decentralized system such as the Blockchain. Instead, everyone on the network owns this data. Therefore, bitcoin could be the solution for the discussed banking problems [10].

Transparency: In the Blockchain, one of the most interesting and misunderstood concepts is “transparency”. Here through complex cryptography, a person’s identity is concealed and identified only by their public address. So if you were to look up the transaction history of an entity, instead of seeing “2NA3cgsKPRAxzy8pvEMFpvtL4PacWr6MYK sent 5 BTC”, you would not see “Rao sent 5 BTC”. So while the individual’s real identity is safe, you can still see all the transactions conducted via their public address. Never before has this degree of accountability existed within the financial sector. It adds that the degree of transparency that some of these largest organizations need is extra and much needed [30].

Immutability: In the context of the Blockchain, immutability means that it cannot be tampered with after anything has been entered into the Blockchain. Since the Blockchain is a linked list containing information and a hash pointer pointing to its previous block, thus forming a chain, that approach makes blockchains so incredibly accurate and revolutionary [5].

No expense of a transaction: Although an infrastructure cost is associated, a blockchain carries no transaction cost. For example, the Bitcoin concept not only can transfer and store money, but it can also substitute all procedures and business models that rely on charging a fee for a transaction or any other operation charges between two parties [17].

Abstraction: Abstraction plays a vital role in the Blockchain. On top of the Blockchain, it provides application interfaces that offer a platform to use Blockchain without having detailed knowledge of the blockchain technique. You can install this app on your computer or mobile device, or it can be hosted on a third-party website. For example, Bitcoin wallet software creates and stores private and public keys that enable users to retain control of the bitcoins. The application layer includes an understandable interface that allows users to keep track of their transactions [3].

4 Types of Blockchains

The most important need for a blockchain is to carry out information transactions via a secure network. But how individuals use Blockchain and distributed ledger technologies differs from case to case. There are primarily four types of blockchains; Public, Private, Consortium, and Hybrid Blockchain. Each of the four forms of Blockchain is comprised of a cluster of nodes (i.e., users) connected via a peer-to-peer network. Each node in the network maintains an updated copy of the shared ledger. Each node is capable of verifying transactions, authorizing or receiving them, and constructing blocks [13].

4.1 *Public Blockchain*

As the names imply, Public Blockchain is freely available and has no limit on who could participate or who can be a Validator. No one in Public Blockchains has complete control over the network. That guarantees data protection and helps immutability because a single individual cannot control the Blockchain. Therefore, a public blockchain is a non-restrictive, less-permission-distributed ledger framework. Anyone with an internet connection can register to become a blockchain platform's authorized participant (node) and a member of a blockchain network. A user (node) that is a member of the public Blockchain may access both current and historical data, validate transactions, or do proofs of work for the received block, as well as engage in mining operations [7].

The authority on the Blockchain is equally divided between each node on the network, and, as a result, Public Blockchains are considered to be completely distributed. One of the important applications of public blockchains is to mine and trade cryptocurrencies. Bitcoin, Ethereum, and Litecoin blockchains are examples of some popular public blockchains. Public blockchains are largely protected when users strictly obey security rules and methods. However, it is only troublesome if the participants do not follow the safety precautions sincerely [19].

Advantages of Public Blockchain

- There is no need for participants (nodes) to think about the reliability of the others. In this case, one node does not need to personally trust the other nodes since the proof-of-work mechanism is responsible for validating each transaction. Therefore, one participant can blindly rely on public blockchains without feeling the need to trust individual participants.
- The public network can have as many users or nodes as possible, making it a secure network. The wider the network, the more records are circulated, and the harder it is for hackers to access the entire network. Besides, the transaction verification and proof-of-work will be performed by each node, making each transaction and

block valid. A public blockchain is even safer than private due to these practices and thoughtful cryptogenic encryption techniques.

- The public blockchains are open for all participants, and the data are also transparent. Copies of blockchain information (digital ledgers) are accessible at any registered node. As a result, blockchain technology is completely transparent and open. Nobody discloses a fictitious transaction or conceals an existent one, since each node maintains an up-to-date copy of the database at all times.

Disadvantages of Public Blockchain

- The number of transactions per second on a public blockchain is really low. This is because it is a big network with several nodes, and each node must spend time validating transactions and performing proof-of-work. That is why public blockchains such as Bitcoin can only process seven transactions per second, whereas the Ethereum network can handle fifteen transactions per second (TPS). On the other hand, a private network such as Visa operates at a pace of 24,000 TPS, demonstrating a huge difference in transaction processing and execution speed.
- As public blockchains have a slow processing rate, this often creates scalability problems. And the more we try to maximize the network size, the slower it is going to get. Solutions like Bitcoin's Lightning Network, however, are helping to resolve this problem. It preserves the transaction rate as we increase the network size.
- Because specialized systems (hardware components) are required to run a special algorithm, the proof-of-work process is highly energy-consuming. It is a matter of concern, both from an environmental and economic point of view. Test-of-work equipment is costly and uses a lot of resources. There is no question that the software needs to generate energy-efficient consensus processes.

4.2 Private Blockchain

The Private Blockchain is also known as the Permissioned or Restrictive Blockchain. The Private Blockchain has prohibitions on who can access and participate in the transaction and validation. Only the pre-chosen individuals have the authorization to access that Blockchain. These individuals are selected by the respective authority and are granted permission by the Blockchain developers during the construction of the Blockchain application. Assuming there is a need to assign new users permissions or revoke existing users' permissions, the Network Administrator can take care of this [7].

Thus, private Blockchain works only in a closed network and is typically used by an association or corporation where only targeted respondents participate in a blockchain network. The level of protection, authorizations, approvals, accessibility is in the control of the managing organization. Private Blockchain networks are used for voting, supply chain management, digital identity, asset ownership, etc.

Advantages of Private Blockchain

- Compared to public blockchains, private blockchain transactions occur at a higher speed. That means, in the case of private blockchains, the TPS rate is higher. This is because, as opposed to a public network, a small number of nodes operate in a private network. This fastens all the nodes in a network with the consensus or authentication process of a transaction. The rate of inserting fresh transactions into a block is also rapid. Private blockchains can enable the transactions at a rate of up to thousands or hundreds of thousands of TPS.
- As per organizational requirements, they can choose the size of their private Blockchain. For example, the organization can easily deploy a blockchain of only 40 nodes or any number. Then, if more nodes need to be added, they can do so easily after expansion. This makes private blockchains very flexible because, without much effort, it provides the organization with the ability to scale up or down the size of its network.

Disadvantages of Private Blockchain

- Private Blockchains are not truly decentralized, since private blockchains require a central management system to work properly. The central management system has all of its control and administrative privileges. It permits a connection of a new node to the network or determines the degree of access to the information stored in the Blockchain. That is one of the main drawbacks of the private Blockchain and goes against the core principle of distributed ledger technology.
- It is difficult to gain trust within the private Blockchain since the centralized nodes make the last call.
- Because a private blockchain network has fewer nodes or users, the probability of a security breach is higher. If one of the nodes gains access to the central management system, all of the nodes in the network can be accessed. For a node, this makes it easier to hack the entire private Blockchain and misuse the data.

4.3 Consortium Blockchain

Some nodes in Consortium Blockchain monitor the consensus mechanism, and some other nodes may be allowed to engage in transactions. The Blockchain Consortium is like a Public and Private Blockchain combination. It is public because various nodes share the Blockchain; and private as well, because the nodes that can access the Blockchain are limited. It is, therefore, partly public and partly private.

In other words, the consortium blockchains are semi-decentralized ledger forms. Furthermore, more than one organization performs within a consortium-blockchain network. Therefore, the feature is contradictory to a private blockchain, which a single organization manages. Several organizations together can serve as participants (nodes) in a consortium blockchain to exchange information or do mining. Consortium blockchains are usually used by banks, service providers, and government bodies.

4.4 Hybrid Blockchain

A hybrid blockchain is a network that combines public and private ledgers. It combines the functionality of both types of blockchains, allowing for the provision of both a private permission-based and a public permission-less system. Users may control who has access to the data stored on the Blockchain in such a hybrid network. Only a subset of the data or documents on the Blockchain may be made public, while the remainder is kept secure on the private network [4].

The hybrid blockchain system is scalable, allowing users to enter a private blockchain while simultaneously accessing numerous public blockchains. Typically, a transaction within a private network of a hybrid blockchain is evaluated by other members of that network. However, users may also submit it to the public Blockchain for approval. Public blockchains enhance hashing and increase the number of nodes available for authentication. This would increase the blockchain network's dependability and transparency. Dragonchain frequently makes use of hybrid blockchains [27].

5 Opportunities for Blockchain Technology in IoT

Blockchain has been applied for different internet-based services in banking, financial, healthcare, Identity management, Insurance, Music, real estate, supply chain, voting & other allied services and has achieved multiple benefits. Intelligent contract services help to carry out financial transactions without an intermediary. It has the ability to automatically handle shares, cash, settlements, and claims [4, 12, 27]. Few use cases and opportunities of blockchain applications are as follows.

5.1 In Banking Sector

The fields in which Blockchain can be used in the banking sector are capital market transactions, monitoring of consortium accounts, cross-border transfers, FX trading, trade finance, etc.

Capital market transactions: Different parties such as exchanges, central counterparties, Central Securities Depositories (CSDs), brokers, custodians, and investment managers are involved in Stock Market Dealing, and they must maintain their ledgers based on the messages exchanged between them. The ledgers must be up-to-date in order to complete the transaction and require intermediate beneficiaries for cash management. It could lead to delay and require potential costs for the final settlement. Blockchain plays a vital role in each and every stage of the exchange, such as pre-trade and post-trade. The Blockchain system makes it simpler to verify Know Your Customer (KYC) and repeatedly prevents several numbers of similar checks.

Transparency and verification of holdings and reduced exposure to credit are given. It ensures more open and stable real-time transactions at the trading stage and provides automated reporting.

Monitoring of consortium accounts: The avoidance of the diversion of funds is the main concern of banks today. The borrower transfers funds from one bank to another, and the banks are not aware of the final use of the funds. Because of the non-existence of the central body, the safe and accurate monitoring of the movement of money between different accounts held by the borrower through different banks and financial institutions has not been operationally feasible; it has thus become one of the challenging areas for banks. An integrated approach between banks and financial institutions is required, enabling them to track money movement and detect process anomalies. By allowing banks and financial institutions to have visibility of the money movement and tracking the end-use of borrowed funds, Blockchain will help solve the issue, thereby helping to improve the monitoring mechanism.

Cross-border transfers: The processing of foreign payments or cross-border payments requires several steps, and it is very difficult to escape from cyberattacks in this course of action. Under the Blockchain, Ripple technology is a distributed ledger used by banks to make foreign transfers simpler and quicker and safe and stable.

FX trading: Different records of currency exchange for sellers, buyers, clearers, brokers, and various third parties are required in the current banking system, and continuous reconciliation across multiple systems is required. Multiple trade records can be extracted using Blockchain for all these actors, and a common view of trade can be offered that frees up resources at the back and mid-level, leading to continuous reconciliation across multiple structures.

Trade finance: Companies introduce Blockchain in trade finance to replace paper-based letters of credit for distributed ledgers. That helps all parties involved in the transaction: exporters, importers, and banks, to exchange information on their network. Without the participation of a third party, a trade agreement may be implemented automatically. From days to hours, it reduces time.

5.2 *In Financial Services*

With digital innovation in the financial sector, examples of Blockchain in foreign payments have already been introduced, benefiting banks in terms of cost savings and shortening processing times. The cryptocurrency was also initially developed worldwide to side-step key control systems. It will open up opportunities for creative legalized landscapes and structures and even more customer-centric and user-friendly exchange and business models to switch to the Blockchain for financial solutions.

The following are a few uses and use cases in financial transactions:

- Cross-border transactions are one of the world's most common blockchain applications. The flow of funds in the centralized system has always been slow and

costly using conventional transaction modes. Verification and processing of cross-border transactions through the use of a decentralized ledger system is a matter of seconds through different time zones.

- Software for smart contracts helps investors to keep smart bonds. Smart bonds are the electronic bond contracts that Blockchain uses for its registration services. These also allow transactions to be settled instantly.
- Using the Blockchain Point of Sales method, merchants and consumers can recognize cryptocurrency as payment. That helps to eliminate unnecessary merchant services and expensive transaction fees for cards. It can also help the management of money and its analysis.
- Using distributed ledger systems, Blockchain allows banks and financial institutions to lend better and borrow cash. It is also possible to make inter-bank borrowing and lending possible, rapid, transparent, seamless, reliable, verifiable, and stable.
- Blockchain aims to reduce the cost of stock exchange share trading and offers an entirely new and creative way to exchange assets without intermediary on the blockchain network. Smart contracts are used without the intervention of any third party to establish the purchase and sale of a security for the investor.
- Auditors can be benefited using Blockchain, as it will assist them to check the specific and material documents and data behind the financial statements and help save expense and time. Distributed ledger technology could allow the integrity of electronic data and files to be demonstrated. The hash string idea is one of the most creative methods to carry the auditing process to real-time.

5.3 In Healthcare

The healthcare sector has been completely reshaped by distributed ledger technology that stores data in an immutable way and updates information in real-time. In this landscape, the conventional models are seen to be extremely inefficient in terms of offering quality healthcare that is accessible for individuals in nature. Healthcare apps focused on Blockchain are ready to be used and are changing healthcare institutions around the world. As the Blockchain works to increase transparency and efficiency, the healthcare system is connected to multiple parties, and patients benefit. The regulatory framework has now become easier to handle in the healthcare system and auditing. Improvement can be seen in the use of advanced technologies in business activities. With the aid of this advanced technology, the conventional or modern healthcare system is sluggish and costly and often requires multiple intermediaries in the system; all such problems are solved.

Blockchain could revolutionize the healthcare industry in many ways:

- Different healthcare systems should work together and cohesively across organizational boundaries to provide more advanced and reliable healthcare facilities.
- Blockchain helps create a “patient-first” ecosystem in which people can handle and store their data and knowledge about a “permitted” blockchain category.

- Blockchain offers a function of immutability in which records and data are unalterable. When each patient has an immutable log, the information is evidence of progress, consistency is definite.
- Decentralized storage of data and information and the payment platform used is inevitably more reliable. As it is built on cryptography and based on asymmetrical private key schemes to encrypt transactions and data, Blockchain data and blocks are difficult to hack.
- When all doctors have access to reliable and unaltered data and information, the Blockchain would have clarity in the healthcare system.

5.4 In Identity Management

Blockchain also changes the way identity management is carried out around the globe. It helps to monitor and manage digital identities safely and successfully, which prevents data leakage and fraud. In any sector, whether it be healthcare, insurance, banking, national security, online retailing, citizenship documents, entry to a bar, or anywhere else, identity verification and authentication are required. Blockchain could revolutionize identity management in several aspects:

For any nation, state, or organization, data accuracy is of paramount importance. In various business activities, real-time data storage using Blockchain can be analyzed and enhanced. In terms of data protection, this will also add trust.

Identity management using Blockchain can help people vote, file their income tax returns, more effectively and safely execute various other procedures. Due to the preservation of government validated IDs using distributed ledger technology, it can also support virtual citizenship authentication. In order to streamline all communications between citizens and the government, all government transactions can be transferred to Blockchain using e-residency identity management.

It is possible to connect the digital identification card to the blockchain data, and this will serve as a temporary ID card when entering a new country. This would lead to smoother immigration services. Travelers can also connect their debit/credit cards and monitor their account behavior, whereas only account holders can be allowed access to avoid theft and fraud.

5.5 In Insurance Sector

By improving business processes and exchanging data with better performance, protection, and accountability, Blockchain is transforming the insurance industry. It uses smart contracts on peer-to-peer networks to carry the policy change from manual to automate into the insurance sector, thus removing the conventional distribution system. Various incentives can be paid out by insurance providers and people seeking insurance using Blockchain. With the aid of decentralization, underwriting,

settlements, claims, and reinsurance processes can be simplified by the insurance industry. This technology would provide better security since the data is not stored in any centralized location and is not managed by any single agency, thereby offering a higher degree of privacy and cost savings.

Blockchain technology offers benefits to different verticals of insurance:

- Blockchain technology not only enhances health benefits but can also change healthcare providers.
- In order to reduce the paperwork, make signing simpler, storing data related to prior repairs, and damage to a car in an immutable and distributed way, the auto insurance industry will benefit, resulting in cheaper quotes and quicker settlement of accident claims.
- Distributed ledger technology can be used in life insurance to connect various cords in life insurance, including insurance providers, insurance companies, funeral homes, beneficiaries, government, etc. Insurance firms can automate the entire processing process with the aid of smart contract technology and can run efficiently with greater productivity with decreased time and resources on operations.
- Travel insurance may also be vertical insurance that uses Blockchain to cover the traveler without the need to make regular calls to the airline's business in case of flight delay.

5.6 In Music Industry

The music industry was transformed and musicians were empowered by Blockchain. It helps to streamline the music's ownership rights and helps to transparently offer equal pay to the artists for their work.

In the music industry, blockchain technology provides many advantages:

- Blockchain provides artists with the means to use smart contracts to share revenue. The smart contract will simplify the song/album contract parameters and release funds accordingly and share revenue in a clear and real-time manner between musicians, managers, etc.
- In the relationship between fans and artists, Blockchain will bring transformation. To purchase music directly, consumers will be able to engage in the tokenized community and will also participate in different surveys, competitions and connect in a meaningful way with the artists.
- The music industry will profit greatly from decentralization because there will not be any central repository where the data and content will be stored. It will help to provide the music industry with a new environment that removes intermediaries and third parties in the process, enabling direct distribution that empowers artists in different ways. It will provide streaming channels for decentralized music in the industry.

- Copyright problems have always been one of the greatest challenges to the development of corporations, musicians, and the music industry. Blockchain offers a greater level of accountability for copyright validation and authentication and provides digital and open rights management.

5.7 In Real Estate

By connecting buyers and sellers, Blockchain may assist in developing a new business model. This technology would lower the real estate investment barrier. With this revolution in the real estate market, there will be a new paradigm of land ownership and rental contracts.

Via a smart contract, the Blockchain real estate platform will cut inspection expenses, registration and loan fees, and property taxes as well. Blockchain may be used to modify the system of rental property payments. With the use of Blockchain, tenants can be safe with all stakeholders, including owners.

Real estate is a fully paper-based industry, so the real estate sector can benefit greatly in terms of operational performance, data storage, and record maintenance with the aid of Blockchain. With the aid of Blockchain and distributed ledger technology, the real estate industry will carry out its essential operations such as payment, title/ownership transfer, escrow, etc. to build outstanding productivity and cost savings.

The most advantageous aspect of real estate is the elimination of fraud, quicker transactions, and increased privacy. In property title management, Blockchain plays a significant role and allows better monitoring of ownership information.

5.8 In Supply Chain

Global trade is a response, rather than a coordinated expansion, to changing needs. With manufacturing processes taking place across the globe and the need for supplier accountability, supply chains are necessary. With real-time monitoring of products and especially attracting businesses with multiple supply chains, Blockchain is ideally suited to supply chain management.

Every inefficient and incompetent supply chain would be removed with the aid of Blockchain. With the support of blockchain-based supply chain solutions that provide end-to-end decentralized processes through distributed ledger technology and digital public ledger, businesses are being transformed.

Without logistics, freight, trucking, storage, and other transport forms that we use to transport goods, the supply chain cannot be addressed. There is a clear need for streamlining and transparency of the system, which can only be accomplished with distributed ledger technology.

5.9 In Voting

Three-quarters of the world's countries are democratic and rely on the consensus of the electorate to elect officials. Sadly, the voting systems at present are unreliable and vulnerable to manipulation. To recognize the rationality of individual people, Blockchain will strengthen the system. Correspondingly, the decentralized ledger to store voting data via Blockchain implies that a centralized authority does not control the outcome.

6 Risk and Challenges of Blockchain in IoT

The Blockchain is still in the initial phases of development, and there are several distinct forms of potential barriers. The types of barriers are internal and external, including those relevant to technical issues with the underlying technology, current business robberies and controversies, public opinion, government policy, and technology's mass acceptance [8, 23, 24].

6.1 Decentralization

When it comes to private blockchains, decentralization is approached differently. Because everyone on the network is identified, it does not matter if just a dozen nodes manage the network. This can be problematic when a company like "Facebook" tries to build a global cryptocurrency Libra on a private network with a limit of 100 participants to start with. Only completely decentralized blockchains are immune to tampering and censorship, and only a few examples of genuinely decentralized blockchains are accessible so far.

6.2 Energy Consumption

To verify transactions and maintain confidence to connect them to the network, Blockchain technology operates on the proof-of-work mechanism. To solve complex mathematical puzzles, this mechanism needs a great deal of computing power to process, validate, and most importantly, protect the entire network.

6.3 Image Problem

There is an image problem with Blockchain. In the minds of many, Blockchain is too related to cryptocurrencies. Crypto, in particular, has a negative reputation surrounded by fraudsters, hackers who use technology for illegal activities. This bad reputation represents the entire blockchain technology system and makes individuals think seriously twice before implementing it.

Members of the public must grasp the distinction between bitcoins, other cryptocurrencies, and Blockchain until general acceptance is feasible. One should realize that cryptocurrencies, among many others, are only one application of blockchain technology. That would help to reduce the often detrimental effects and contribute to an increased desire to use the program.

6.4 Interoperability

The major challenge that needs to be solved is interoperability, as this is one of the main reasons why organizations are still not implementing this technology. Some blockchains run in silos and do not connect with other peer networks since they cannot send or receive data from another blockchain-based framework.

6.5 Lack of Regulatory Clarity and Good Governance

Regulatory clarification about the underlying blockchain technology, which is a big roadblock for mass adoption, is also lacking. Regulations have always failed to keep up with technological advancements. For the Blockchain, this is also the case. One of the challenges (which was also one of its original motivations) of the blockchain solution is that it eliminates oversight.

As a means of exchange, many companies are producing blockchain technology. However, there are not any clear rules on it right now. So when it comes to the Blockchain, no one follows any particular rules, so there is still no protection.

Some areas need regulatory support, such as the smart contracts listed earlier. It prevents adoption and investment in the blockchain industry if the regulations do not cover smart contracts.

6.6 Lack of Standardization

There is no standardized norm yet, despite a wide range of networks that exist. Issues such as interoperability, increased costs, and complicated processes emerge

from the lack of standardization, rendering mass adoption an unlikely mission. Since blockchain technology does not follow any standard version, it also serves as an obstacle to the entry of new developers and investors.

6.7 Lack of Talent

Without delay, the demand for blockchain professionals is rising, but high-quality talents can be seen as a significant difficulty in adopting this technology. Despite considerable accomplishments, most of the crowds see Blockchain as a developing area. While there is a strong demand for Blockchain developers, an acute shortage of blockchain experts and developers is a major concern for all organizations. The lack of professionally trained and experienced developers to handle and overcome the complexities of peer-to-peer networks further contributes to a slow rate of growth.

6.8 Organizational Challenges

Various organizational problems restrict the corporate use of blockchain technology.

Lack of awareness and understanding: A lack of knowledge of technology and a widespread lack of understanding of how it works is the main challenge for blockchain-related businesses, especially small and medium ones. Many businesses do not know what the Blockchain is or what they can do. That has a lot to do with the domination of blockchain technicians and their excessive approach to technology.

Productivity paradox: There is a phenomenon known as the blockchain paradox. The increased speed and dependability with which blockchain networks can. There is a phenomenon known as the blockchain paradox. The increased speed and dependability with which blockchain networks can conduct peer-to-peer transactions comes at a high aggregate cost, which is more than for other types of Blockchain. This inefficiency occurs because, in an effort to be the first to find a solution, each node performs the same tasks as any other node on its own copy of the data.

Lack of cooperation: The Blockchain adds the most value to organizations when they collaborate on “shared pain or shared opportunity” areas. However, many present systems are self-contained: organizations build their own blockchains and software to operate on top of them. As a result, in each given business sector, several chains are built to meet a variety of distinct demands by a variety of distinct organizations. This defeats the purpose of distributed ledgers, ignores network effects, and may be less dependable than existing alternatives.

6.9 Scalability

The scalability of the Blockchain is the key problem related to its adoption. Although transaction networks can process thousands of transactions per second without any malfunction, there is a remarkable slowdown in transaction processing when it comes to Bitcoin (approximately 3 to 7 transactions per second) and Ethereum (15 to 20 transactions), rendering Blockchain unviable for large-scale applications.

6.10 Security and Privacy Challenges

Although cryptocurrencies provide pseudonymity, many future blockchain implementations require that intelligent transactions and agreements be unquestionably connected to established identities, posing critical concerns about the privacy and protection of the data stored and accessible on the shared ledger.

Many businesses now operate with privacy laws controlled by legislation. With confidential details, their customers trust them. But if any of this data is kept in a public ledger, it will not really be private anymore. Private or Blockchain consortiums may operate here. Restricted access would be granted to you, and all your personal details would remain private as they should.

Another critical issue is security. Only a few situations, however, have robust mechanisms in place to address this. While blockchains provide a higher level of security than traditional computer systems, hackers may still compromise blockchain-based applications, networks, and businesses.

6.11 Technical Challenges

Developers are aware of the issues, as evidenced by a wide range of replies to the problems posed, as well as active debate and coding of potential solutions. Insiders have varying degrees of trust in whether and how these challenges can be overcome in order to move the blockchain industry forward to the next stage of development. Some claim the Bitcoin blockchain would be the de facto norm since it is the incumbent; with the technology most widely distributed and such network effects, it cannot help but be the standardized foundation. Others create various modern and distinct blockchains (such as Ethereum) or systems that do not use a blockchain (like Ripple). One major problem with the underlying Bitcoin technology is scaling up from the current maximum cap of 7 transactions per second.

6.12 The Ecosystem

The other difficulty is that it needs a decentralized blockchain ecosystem that supports distributed products and services. That involves decentralized cloud storage, decentralized archiving, decentralized networking, and decentralized domain name servers (currently being built by businesses such as Ethereum and the InterPlanetary File System). Most of these technologies have not been fully developed yet, resulting in major risks for anyone who wants to work with Blockchain and develop fully decentralized and independent organizations.

6.13 The Vested Interest of Incumbent Parties

Current rules are by far the most significant impediment to blockchain innovation, since they “protect incumbents and their vested interests in disruptors”. ‘Digitization (of information) occurs within a so-called “heavy regulatory zone. Given governments” long-established jurisdiction to protect consumer and property rights, this is not unusual.

Blockchain presents new problems for regulators aiming to safeguard customers and markets, but the rigidity with which authorities in the world’s leading countries have addressed Blockchain has helped to hinder innovation and progress.

7 Summary

Via the use of sensors and other edge devices and infrastructure, IoT is changing the way businesses work. That is a big challenge for companies that need to secure data at all levels of the IoT ecosystem. Data security has become increasingly complex, with the number of connected devices rising multifold every year. In an IoT scheme, Blockchain helps combat security breaches.

There is no question that the IoT and blockchain technology will have a significant impact in the automated futuristic world. While IoT use is rapidly growing, it is rife with scalability, stability, privacy, and honesty. While Blockchain was originally built to manage cryptocurrencies, to enhance it, its decentralized existence, higher protection, honesty, and privacy have led to the integration with IoT.

Beyond its initial implementation areas, the properties of its protection, privacy, traceability, inherent data provenance, and timestamping have seen its adoption. The Blockchain itself and its variations are now used, whether human-to-human communication or machine-to-machine, to protect any kind of transaction. In particular, with the global advent of the Internet of Things, its adoption seems to be stable. In terms of ensuring data redundancy and survivability, its decentralized deployment across the already developed global Internet is also very attractive.

The Blockchain's potential benefits extend beyond political economy, it applies to humanitarian, political, social, and scientific areas, and specific groups are now leveraging blockchain technology to solve real-world problems. The Blockchain may be used for any kind of asset register, warehouse, and distribution, covering all financial, commercial, and money sectors; hard assets (physical property); and intangible assets (ideas, reputation, intention, health data, votes, etc.). For instance, blockchain technology may be used to enact decentralized cloud functions that historically mandated administration by jurisdiction-bound entities to fight oppressive political regimes. Other sectors and classes of the industry can be freed from skewed regulatory and licensing schemes subject to hierarchical power structures and the influence of strongly supported special interest groups on governments, enabling new disintermediation business models beyond those situations in which the public interest must transcend government power structures. In addition to economic and political benefits, the Blockchain could act as the archive of public records for whole organizations, including documenting all data, activities, identities, and properties.

Scalability, as well as a lack of speed, skill, and standards, may have a negative impact on the development of new organizational models, such as decentralized autonomous organizations, both in the implementation and development of new blockchain applications. Yet, amid these difficulties, almost every industry has encountered hundreds of new applications that implement distributed ledger technologies and are already benefiting from this fundamental technology. This will require more computing power than IoT devices already suffer from. Therefore, further study is required to resolve this current constraint.

References

1. Ahmed MS (2021) Designing of internet of things for real time system. Mater Today: Proc <https://doi.org/10.1016/j.matpr.2021.03.527>
2. Azbeg K, Ouchetto O, Andaloussi SJ, Fetjah L (2021) A taxonomic review of the use of IoT and Blockchain in healthcare applications. IRBM.<https://doi.org/10.1016/j.irbm.2021.05.003>
3. Breidbach CF, Tana S (2021) Betting on Bitcoin: How social collectives shape cryptocurrency markets. J Bus Res 122:311–320. <https://doi.org/10.1016/j.jbusres.2020.09.017>
4. Centobelli P, Cerchione R, Esposito E, Oropallo E, Ghode DJ, Jain R, ... Yadav V (2020). Architecture to enhance transparency in supply chain management using Blockchain technology. Procedia Manuf 51:1614–1620.<https://doi.org/10.1016/j.promfg.2020.10.225>
5. Chen G, Xu B, Lu M, Chen N-S (2018) Exploring blockchain technology and its potential applications for education. Smart Learn Environ 5(1). <https://doi.org/10.1186/s40561-017-0050-x>
6. Choi W, Kim J, Lee SE, Park E (2021) Smart home and internet of things: a bibliometric study. J Cleaner Prod 301:126908.<https://doi.org/10.1016/j.jclepro.2021.126908>
7. Dutra A, Tumasjan A, Welpe MI (2018) Blockchain is changing how media and entertainment companies compete. Mit Sloan Manag Rev 60(1)
8. Galvez JF, Mejuto JC, Simal-Gandara J (2018) Future challenges on the use of blockchain for food traceability analysis. TRAC, Trends Anal Chem 107:222–232
9. Garg K, Goswami C, Chhatrawat RS, Kumar Dhakar S, Kumar G (2021) Internet of things in manufacturing: a review. Mater Today: Proc. <https://doi.org/10.1016/j.matpr.2021.05.321>

10. Gupta V, Knight R (2017) How Blockchain could help emerging markets leap ahead. Harv Bus Rev, MAY, 1–6
11. Johnson A (2017) An introduction to Blockchain. Darden Business Publishing, 1–15
12. Kimani D, Adams K, Attah-Boakye R, Ullah S, Frecknall-Hughes J, Kim J (2020) Blockchain, business and the fourth industrial revolution: whence, whither, wherefore and how? Technol Forecasting Soc Change 161:120254.<https://doi.org/10.1016/j.techfore.2020.120254>
13. Kopyto M, Lechner S, von der Gracht HA, Hartmann E (2020) Potentials of blockchain technology in supply chain management: long-term judgments of an international expert panel. Technol Forecasting Soc Change 161:120330.<https://doi.org/10.1016/j.techfore.2020.120330>
14. Kumari A, Gupta R, Tanwar S (2021) Amalgamation of blockchain and IoT for smart cities underlying 6G communication: a comprehensive review. Comput Commun 172:102–118. <https://doi.org/10.1016/j.comcom.2021.03.005>
15. Larios-Hernández GJ (2017) Blockchain entrepreneurship opportunity in the practices of the unbanked. Bus Horiz 60(6):865–874. <https://doi.org/10.1016/j.bushor.2017.07.012>
16. Lone AH, Naaz R (2021) Applicability of Blockchain smart contracts in securing Internet and IoT: a systematic literature review. Comput Sci Rev. Elsevier Ireland Ltd. <https://doi.org/10.1016/j.cosrev.2020.100360>
17. Murck P (2017) Who controls the Blockchain? Harv Bus Rev
18. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. Retrieved from www.bitcoin.org
19. Pereira J, Tavalaei MM, Ozalp H (2019) Blockchain-based platforms: decentralized infrastructures and its boundary conditions. Technol Forecast Soc Chang 146:94–102. <https://doi.org/10.1016/j.techfore.2019.04.030>
20. Ramamoorthi S, Muthu Kumar B, Mohamed Sithik M, Thinesh Kumar T, Ragaventhiran J, Islabudeen M (2021) Enhanced security in IOT environment using Blockchain: a survey. Mater Today: Proc. <https://doi.org/10.1016/j.matpr.2021.03.346>
21. Saxena S, Bhushan B, Ahad MA (2021) Blockchain based solutions to secure IoT: background, integration trends and a way forward. J Netw Comput Appl. Academic Press. <https://doi.org/10.1016/j.jnca.2021.103050>
22. Treiblmaier H (2018) The impact of the blockchain on the supply chain: a theory-based research framework and a call for action. Supply Chain Manag Int J 23(6):545–559. <https://doi.org/10.1108/SCM-01-2018-0029>
23. Upadhyay N (2020) Demystifying blockchain: a critical analysis of challenges, applications and opportunities. Int J Inf Manag 54:102120. <https://doi.org/10.1016/j.ijinfomgt.2020.102120>
24. Venkatesh VG, Kang K, Wang B, Zhong RY, Zhang A (2020) System architecture for blockchain based transparency of supply chain social sustainability. Robot Comput Integr Manuf 63:101896. <https://doi.org/10.1016/j.rcim.2019.101896>
25. Weili Z (2020) Industrial park innovation ecosystem based on FPGA and internet of things. Microprocess Microsyst, 103463.<https://doi.org/10.1016/j.micpro.2020.103463>
26. Weiss M, Corsi E (2018) Bitfury: blockchain for government. J Harv Bus School, 1–29
27. White R, Marinakis Y, Islam N, Walsh S (2020) Is Bitcoin a currency, a technology-based product, or something else? Technol Forecasting Soc Change 151:119877.<https://doi.org/10.1016/j.techfore.2019.119877>
28. Yi H, Lin W, Huang X, Cai X, Chi R, Nie Z (2021) Energy trading IoT system based on blockchain. Swarm Evolut Comput 64:100891.<https://doi.org/10.1016/j.swevo.2021.100891>
29. Yoffie DB, Woo AK (2017) Note on Blockchain and bitcoin. Harv Bus School
30. Zelbst PJ, Green KW, Sower VE, Bond PL (2019) The impact of RFID, IIoT, and Blockchain technologies on supply chain transparency. J Manuf Technol Manag 31(3):441–457. <https://doi.org/10.1108/JMTM-03-2019-0118>

Challenges and Issues in Blockchain-Based IoT Services



Arunima Sharma and Ramesh Babu Battula

Abstract In this chapter, we present a couple of challenges and problems in Blockchain (BC)-based Internet-of-Things (IoT) applications, where considering the IoT into unique solution. IoT as distributed data manager, sensing solution, and advancements could be the right alternative. Among the customary categories of spread record improvements are present in the blockchain. This one uses a distributed way of thinking which passes on better capacity and takes out the single indication of thwarted expectation. In accumulation, blockchain passes on improved safety and information fairness concluded carefully arranged and constancy highlights. The wire of blockchain using IoT can sort out problems of IoT solidified design and then gives a decent procedure to upcoming movements. Hence, the goal of this chapter is to give an extensive conversation of intertwining the IoT framework with blockchain progression. In the wake of introducing the explanation of IoT and blockchain, the part gave a wide conversation of preparation IoT blockchain by featuring how blockchain settled issues of IoT. In addition, late assessments giving the blend of IoT blockchain are likewise introduced. At that point, blockchain by means of a help on behalf of IoT be there talked about to demonstration in what way different highlights of BC innovation can remain carried out, for instance, a help on behalf of different IoT solicitations. This was trailed through future exploration bearings of IoT with blockchain.

Keywords Bitcoin · Blockchain · Ethereum · Internet of Things · Attacks · Pseudonymity

A. Sharma (✉) · R. Babu Battula
Malviya National Institute of Technology, Jaipur, India
e-mail: rbbattula.cse@mnit.ac.in

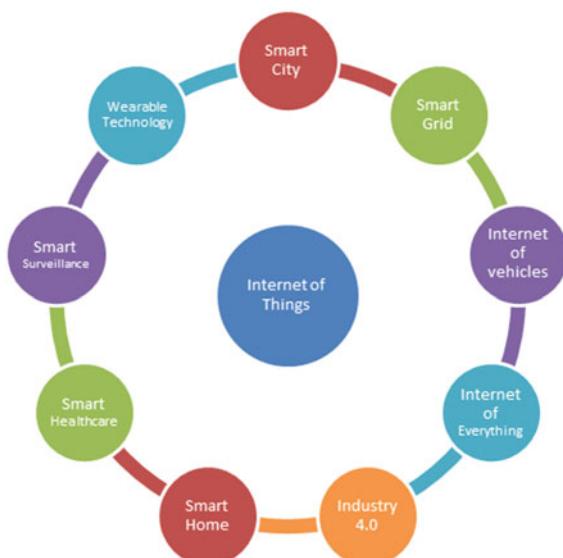
1 Introduction

The Internet of Things (IoT) addresses perhaps one of the main troublesome advances of this century. It is a development trait of the Internet (of computers or digital devices) to mounted and cyber-physical systems, “things” that, even though not undoubtedly processors themselves, by the by have processors inside them. Through an organization of unassertive sensors and interrelated things, records assortment on authenticity and environment can be proficient at a lot advanced level. To be sure, such definite information will improve efficiencies and convey progressed administrations in a wide scope of utilization areas including unavoidable medical care and smart city administrations. Notwithstanding, the inexorably untraceable, dense also inescapable assortment, formulating, and smattering of data among entities isolated subsists brings about honest safety and security worries. According to one point of view, this data can be used to offer an extent of complex likewise, modified organizations that offer utility to the customers. On the other hand, embedded in this data can't avoid being information that can be used to algorithmically assemble a virtual record of our activities, uncovering private lead, and lifestyle plans.

The insurance risks of IoT are exacerbated by the shortfall of key security safeguards in countless the first IoT things accessible. Different security shortcomings have been recognized in related contraptions going from smart locks till smart vehicles.

A couple of trademark attributes of IoT improves his safety and assurance challenges containing: nonappearance of fundamental mechanism, different attack surfaces, heterogeneity in contraption resources, setting careful and situational nature

Fig. 1 Internet of Things (IoT)



of risks, and scale. Normally, security and protection for IoT is accepting a ton of consideration inside the examination local area. An appropriated ability-based admittance control technique is used to control admittance to touchy data. In any case, their proposed technique presents over the top postponements and overheads and might actually bargain client protection. It utilized IPsec and TLS to give validation and protection; however, these strategies are computationally costly and may consequently be wrong for some, asset-restricted IoT gadgets. A security the board strategy is suggested in which appraises the peril of uncovering data to others, notwithstanding, much of the time, the apparent benefit of IoT organizations surpasses the risk of protection misfortune. There is as needs be a necessity for security careful sharing of IoT data without relinquishing the insurance of customers. In rundown, these and a couple of other prior works as of now can't address the recently referenced troubles in ensuring security and assurance for IoT in a broad manner.

The appropriate response may lie in the crucial innovation that underscores arising digital currencies. Bitcoin, the world's initially decentralized advanced money, was dispatched in 2008. Bitcoin is supported by a shared system association which is prepared of its customers' equipment, as Bit Torrent. Likewise, a changing Public Key (PK) is cast-off as client's personality to provide anonymous in addition with insurance. The crucial development after Bitcoin is entitled Blockchain (BC), a changeless freely available report of information got by an organization of shared members. BC is quickly acquiring fame and is being utilized for numerous different applications including smart agreements, appropriated distributed storage, and computerized resources. BC comprises blocks tied all together. Any hub in the distributed organization can decide to be an excavator, an element that is liable for mining blocks to BC by resolving a resource-focused cryptographic conundrum called Proof of Work (POW) [8] and attaching fresh blocks toward BC. Right when another trade occurs, it is imparted to the entire organization. All diggers who get the trade affirm it by supporting the imprints contained inside the trade. Each digger joins the checked trade to its own impending block of trades that are clutching be mined. The vigor of the BC is guaranteed by the way that various diggers measure a solitary exchange. Nonetheless, heartiness includes some major disadvantages as different diggers need to consume their assets for mining something very similar exchange, which thusly likewise expands the deferral. The accompanying striking highlights of BC make it an appealing innovation for tending to the previously mentioned security and protection challenges in IoT:

- **Decentralization:** The shortfall of central control ensures flexibility and generosity by using resources of each participating center and getting rid of many-to-one traffic streams, which in this way lessens deferral and overcomes the issue of a singular sign of disillusionment.
- **Anonymity:** The trademark anonymity oversaw is proper for most IoT use situations where the personality of the customers ought to be kept covered up.
- **Security:** BC understands a safe organization over untrusted parties which is alluring in IoT with various and heterogeneous gadgets.

Nevertheless, getting BC in IoT isn't clear and will expect watching out for the going with essential challenges:

- Mining is particularly computationally focused, while a large portion of IoT devices are resource restricted.
- Mining of blocks is tedious while in most IoT applications low dormancy is attractive.
- BC scales ineffectively as the quantity of hubs in the organization increments. IoT networks are expected to contain an enormous number of hubs.
- The basic BC conventions make critical overhead traffic, which might be bothersome for certain transmission capacity-restricted IoT gadgets.

2 Blockchain (BC)

The world continued utilizing the united designing wherein a central laborer is required toward governor the dealing with besides arranging of jobs till Szabo made decentralized advanced money close to the completion of 1990. Following 10 years, Bitcoin computerized cash was publicized. Blockchain ended up being generally limitless after Satoshi Nakamoto's research paper in 2009. This section offers a detailed view of BC development.

2.1 A Synopsis of Blockchain

BC advancement is among the utmost latest refrains that pulled in the thought of a couple of affiliations and examiners as a result of the multitudinous benefits it gave over existing game plans.

A blockchain is fundamentally a passed on, decentralized, and perpetual record which possesses the data of the numerous trades that reliably occurred within a particular Peer-to-Peer (P2P) organization. On the way to stock a trade in scattered record, utmost of the hubs must save their arrangement. This needs an arrangement framework. The utmost notable plus renowned understanding segments are Proof of Stake (PoS) and Proof of Work (PoW). A social occasion of trades is assembled and consigned a block in the record. A time-stamp what's more, hash work related with every single block is cast-off acquaintance the block with the past block. Thusly, different blocks remain moored organized, and known as BC. The hash work is fundamentally cast-off to support trustworthiness of the block's substance or information. The BC development propels data participating in which each and every partaking customer/hubs in BC network make sure to have a replica of the primary record, so all hubs be present invigorated by way of as-of-late additional trades or else blocks.

There be present numerous explanations for the BC. Intended, for example, Coin base, the world's biggest digital cash interchange, portrayed BC as “a scattered, openly available report that contains the authentic setting of each bitcoin trade.” Similarly, the Oxford word reference characterizes blockchain. It expressed, “a computerized record where exchanges made in bitcoin or another digital money are recorded sequentially furthermore, freely.” These definitions depict the blockchain from cryptographic money’s perspective that doesn’t mirror the truth that blockchain can be used in various areas. Additionally, examining key segments of blockchain conveyed a typical portrayal for the blockchain.

It expressed “a decentralized information base containing consecutive, cryptographically connected blocks of carefully marked resource exchanges, administered by an agreement model.”

2.2 *Sections of Blockchain*

Blockchain development can pass on a couple of reimbursements above present game plans. Here remain many simple aspects of the BC, which minor, block, fuse record, hashing, trade, and understanding frameworks, as represented in Fig. 2. The record stands as a data structure which is exploited to save innumerable varieties of data. Here are basic differentiations among the customary informational collection besides the record. A database structure provisions records as tables with fragments and lines. Also, it used a social manner to address and gather records by interfacing data commencing a couple of foundations.

However, the record remains used toward collection altogether of the trades that remained anytime created utilizing altogether partaking customers cutting-edge association. Moreover, the record remained divided between the participating hubs, consequently every customer takes his individual duplicate of the record.

Block residues among the fundamental pieces of the BC. Every block includes a lot of trades. The blocks remained blinded composed through taking care of an extraordinary hash assessment of the past block in the current block. This association thwarts composed similar like a sequence. The jumble work remains used toward support the statistics trustworthiness of the substance of every block. Generally, the jumble effort remains a calculated issue that the minors want toward break, toward discovery of a block. The inspiration toward custom the complex work remains that this one residue cutting edge and other one residues tough make two indistinct jumbles aimed at two dissimilar electronic statistics. Subsequently, consigning a

Fig. 2 Blockchain structure



distributed motivation aimed at every block can fill in by way of toward deal with perceive the discourage besides moreover endorse this one substance.

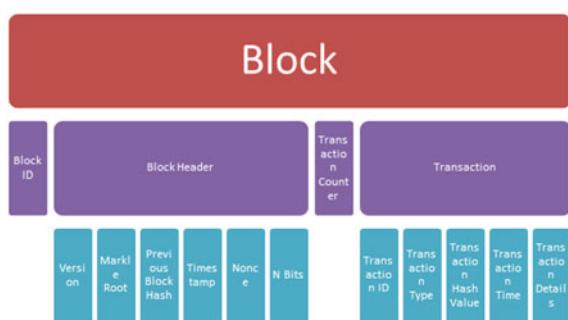
A trade remains the smallest unit of cooperation otherwise movement where a lot of trades remain solidified besides taken care of cutting-edge block. A particular trade can't be added to the block aside from in case the overwhelming mainstream of the sharing hubs cutting edge the BC system archives their agreement. The scope of a trade is huge aimed at minors by way of little trades need fewer authority besides remain less difficult to support. Minors remain PCs/experts that are being undertaken to handle a multifaceted scientific issue (generally, a kind of jumble abilities) to examine another block. Discovering another block is started by conveying new trades to all centers, and a while later every center point syndicates a lot of trades hooked on a block besides attempts toward determining the block's check of work. In case a center point determines a block, the block determination be present conveyed toward altogether of the centers toward remain affirmed.

2.3 Structures of BC

BC can pass on different benefits aimed at various arenas besides solicitations. This novel advancement bonds certain ordinary structures that incorporate

- **Decentralization:** BC remains customarily a dispersed besides scattered environment that remains considering the peer-to-peer correspondence amid passing on centers. The delegation allows using the dealing with control of each and every contributing customer, which reductions lethargy besides kills the solitary sign of disillusionment. This segment vanquishes the solitary sign of dissatisfaction matter (Fig. 3).
- **Transparency:** As opposed toward the united prototypical wherever the dominant laborer remains simply consuming the occupied switch besides permission toward altogether statistics, BC bids a decent side by side of straightforwardness wherein altogether hubs approach every one of the subtleties of the exchanges that consis-

Fig. 3 Block in a blockchain



tently occurred in their organization. Furthermore, every hub has a duplicate of the appropriated record to keep refreshed with changes. Moreover, the shortfall of an outsider expands business benevolence and trust.

- **Immutability:** Amid significant qualities of BC remains the ability of ensuring the exchanges' honesty done delivering unchanging records. Rather than the concentrated model where information honesty is just overseen and saved through the focal position that can remain a risk, the BC expenditures hash works that are crash permitted to interface each block to the past block which keeps up the uprightness of the block's substance. Additionally, blocks set aside in the record cannot ever remain altered just condition maximum of the customers avow that alteration.
- **Better security:** Among the benefits of BC advancement remains that this one gives improved safety above current plans. Through the usage of communal vital establishment, BC gives a secured surroundings besides numerous kinds of outbreaks. Moreover, the understanding instrument gives a reliable in procedure that works on the safety of the BC. Additionally, the deficiency of the solitary sign of dissatisfaction cutting-edge BC advancement that can impact the entire structures gives improved safety completed the united prototypical.
- **Anonymity:** Paying little mind to BC utilizing a record that is circled between all customers, BC gives an obscure character to guarantee the hubs' security. The lack of definition article can be exploited beside isolated vote-based scheme.
- **Cost decline:** As opposed toward the bound together designing wherein the undeniable level besides whole hardware besides programming structure remains expected toward shape the concentrated specialist, the BC advancement diminishes the expenses connected toward appropriate besides supporting gigantic united laborers by way of it uses the getting ready control of giving contraptions.
- **Autonomy:** The capacity to settle on independent choices remains among the highlights that the BC innovation can give. This one permits assembling of novel gadgets that can mark keen also, independent choices. For example, BC highlights counting sealed besides improved safety can remain to assemble improved besides safe self-sufficient automobiles.

3 Internet of Things Using BC

The Internet of Things gotten extraordinary advances that engage fundamental actual items. Together their associated composed done at top, with cutting-edge and create different dissimilar spaces. The abrupt improvement of the Internet-of-Things structure takes opened imaginative potential outcomes in various fields. In any case, the Internet of Things really has a couple of issues that stand like a divider even with the guaranteed dispersal of Internet-of-Things substances. Among these problems remains the shortfall of conviction besides conviction. The present Internet-of-Things fused classical uses a pariah principal position that consumes limitless authority of records variety additionally, getting ready from various Internet-of-Things objects with no indisputable impediments around in what way the assembled statistics be

Table 1 A straightforward examination among BC and Internet of Things

Properties	IoT	BC
Confidentiality	Lack of safety	Guarantees the security of the captivating nodes
Data transmission	IoT devices have restricted transfer speed also, assets	High transmission capacity utilization
Framework	Unified	Dispersed
Adaptability	IoT deliberated to comprise huge number of devices	Unsuccessfully with an enormous group
Assets	Resource confined	Resource devouring
Potential	Low idleness	Tedious
Safety	Issue	Better

there actuality cast-off. Henceforth, the vital expert looks similar a block container aimed at Internet-of-Things customers, which remains a undoubted condition for the vast mainstream of Internet-of-Things maneuvers' possessors.

Of course, BC development passes on decentralized, independent, trust less besides dispersed situation. Trendy separation toward the united prototypical where here remain a couple of problems identified with the solitary spot of frustration, expectation besides safety, the BC exploits a dispersed method toward manage usage the getting ready limits of the general large number of contributing customers which pass on better efficiency and abstain from the single sign of disillusionment. Moreover, BC gives improved safety also statistics decency concluded fixed besides immutability structures. Here remain various similitude besides fluctuations amid Internet of Things besides BC. Table 1 gives a straightforward examination among Internet of Things besides BC.

Organizing the BC development by means of Internet of Things can decide a couple of troubles of the brought together Internet of Things prototypical. Table 2 gives an outline of the tasks of the concentrated Internet-of-Things structure besides in what way organizing BC by means of Internet of Things might manage it.

4 IoT with BC Architecture

Incorporating BC by means of Internet of Things has developed a need toward conquering the problems of the brought together Internet-of-Things engineering besides using incalculable advantages of BC innovation. Executing BC by means of Internet of Things can remain accomplished from multiple points of view. This segment grants a conversation for unique methodologies of coordinating BC by means of Internet of Things in a coated engineering.

Table 2 BC can offer innovative responses for problems of the concentrated IoT prototype

Troubles of concentrated IoT	How BC resolves the issues
Security	BC compromises improved safety by using the public-key foundation which gives additional insurance in contradiction of different assaults. Likewise, it offers an unchanging record that can't be refreshed distinctly with the endorsement of most of contributing clients in the network, which ensures information honesty. Besides, all correspondences between different gadgets are kept up and gotten cryptographically
Adaptability	Among the principle parts of the IoT is the tremendous number of gadgets which continually builds each time. The appropriated and distributed landscape of the BC can give a productive method to give an adaptable method to deal with the steady expansion in IoT gadgets
Mark of failure	The BC innovation gives circulated and decentralized correspondence between taking part hubs which takes out the need for a focal worker to oversee and control handling and correspondence activities. Consequently, in the event that one gadget goes down, this won't influence the whole organization which defeats the single place of disappointment problem connected with the integrated prototype
Address space	The BC takes an enormous area space which licenses circulating addresses to countless maneuvers. The BC gives 160 address space which permits the BC to distribute addresses aimed at a great amount of articles. Stood out from IPv6, BC bids more than 4 billion extra areas
Affirmation and access control	Among the advantages gave by BC development is conveying effective personality the executives that assists with building powerful verification and access control. Additionally, savvy contracts give a few advantages, for example, decentralized verification decides that can be used to give a powerful confirmation model to different IoT gadgets
Data integrity	BC presents a sealed capacity with the end goal that a specific exchange can't be added, altered, or erased just if a large portion of the contributing clients in the organization confirm it. This, thus, ensures information honesty
Susceptibility to manipulation	The BC gives a changeless climate that forestalls the control of information to guarantee information honesty. In the BC, the control or update is as it were affirmed after the arrangement of most of taking an interest clients
Possession and identity	BC has the ability to pass on a reliable, approved character enlistment, possession following and observing. Moreover, it was carried out effectively in different applications particularly in the following and observing merchandise and items
Tractability	The BC development gives versatile surroundings to numerous IoT things over different open-source choices aimed at BC. Likewise, BC can gauge fine to encounter the degree and worth-based capacity of a versatile structure
Expenses and capacity imperatives	The BC gives a distributed engineering wherever a focal position or outsider isn't needed to deal with the interchanges between imparting hubs. This takes into account safer information correspondence and trade. Likewise, no requirement for the expenses of introducing a worker with high programming and equipment abilities

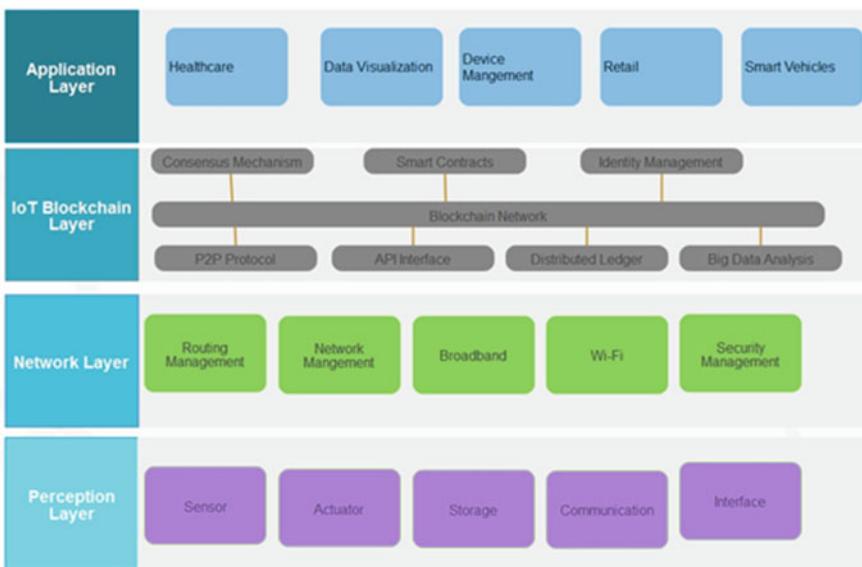


Fig. 4 Engineering of IoT with BC

The basic coated BC by means of Internet-of-Things engineering involves four levels. This one is the Internet-of-Things design levels accumulation BC as a different layer among system besides solicitation levels, by way of demonstrated in Fig. 4.

Before, the primary level remains the observation level that comprises Internet of Things, things besides elements, for example, devices besides actuators that remain utilized toward detecting and seeing the general climate besides gathering pertinent information that can assist us with understanding our environmental factors. At that point, the organization level that accomplishes system besides directing administration empowers entirely Internet-of-Things entities toward be connected besides impart composed preposterous. This level incorporates systems administration besides safety gadgets that empower correspondence besides safety of the executives.

The final additional level is called the Internet-of-Things BC level, which incorporates entirely units that allow numerous structures of the BC advancement toward stand executed cutting-edge Internet-of-Things structure. These structures fuse peer-to-peer correspondence, scattered record, brilliant arrangements, Application Programming Interface (Programming interface), huge data examination, understanding the board, and character the chiefs. P2P shows are needed to engage decentralized correspondence amid numerous Internet-of-Things objects. Moreover, the scattered record remains among the basic structures that every Internet-of-Things contraption resolve grip a duplicate of consequently it might be invigorated by means of variations in records or else uniform instants inside the Internet-of-Things organization. The record can stay made either by means or deprived of approval. The compassion-

ate of record remains overwhelmingly reliant on upon the Internet-of-Things setting besides the amount of center point's cutting-edge Internet-of-Things association.

The Big Data examination unit allows the BC towards the web information stockpiling, preparing since the Internet-of-Things framework make tremendous measures of information. This Information can't be handled by utilizing primary techniques. Also, numerous exchanges are saved in organized methods of records, which will need additional information examination. Keen agreements remain likewise among the significant pieces of BC innovation that cast-off toward empower computerized choices dependent on foreordained conditions.

Ordinarily, a shrewd agreement is an item cipher that tracks by means of BC toward performing a lot of activities at the point when foreordained conditions are met or confirmed. Agreement is likewise among the primary highlights expected to incorporate BC with Internet of Things. It goes about as the focal worker that keeps up the trust between conveying hubs in the organization.

Character classification is utilized to control and recognize different hubs in the Internet-of-Things organization. What's more, the programming interface engages Internet-of-Things uses toward get to BC organizations. The application level remains the highest level that consolidates diverse Internet-of-Things uses besides giving information representation undertakings that make various digitized administrations and help chiefs settle on exact and exact choices dependent on the gathered information from actual Internet-of-Things gadgets.

5 Execution of BC Using IoT

BC was first and foremost utilized for monetary exchanges and cryptographic money where exchanges remain performed moreover put away through altogether hubs' cutting-edge BC system. At that point, BC remains incorporated happening different areas because of the colossal advantages it gives. Among these spaces remain the Internet-of-Things framework. Consolidating BC by means of Internet of Things can give endless advantages to different Internet-of-Things applications. In the meantime, the BC is dispersed besides reliance less, by way of it remains reasonable for Internet-of-Things uses like medical services, keen households, keen city, and intelligent conveyance besides others.

Executing BC cutting-edge Internet-of-Things framework is certifiably not a simple assignment. The chief besides significant advance remains to pick the BC stage that remains received to combine the Internet of Things by means of BC innovation. Ethereum, Hyperledger besides IOTA remain the greatest widely recognized stages that can remain used cutting edge carrying out BC by means of Internet of Things. In addition to the fact that they are open-source stages, they can likewise convey key capacities to associate among chunks, cryptographically secure aimed at the shredding of various exchanges negligibly cutting-edge solitary squares, progressed imprints, agreement, and shrewd agreements.

5.1 Ethereum

Ethereum be present as a versatile BC stage that remained declared in 2013 besides afterward dispatched in 2015. It creates a widespread stage aimed at different BC founded solicitations. It remained basically in light of executing savvy agreements, which remain customized ciphers that remain for all time reserved scheduled the BC besides empower implementing clients' solicitations. Ethereum likewise proposes a dispersed computer-generated mechanism named Ethereum Virtual-Machine (EVM).

Despite the fact that Ethereum depends on savvy gets, the exchanges can keep various kinds of information. This expands the probability for auditability and permits vigorous development for different Internet-of-Things solicitations. Among the disadvantages of Ethereum remains exist with duration in the range of 10–20 sec to lead a square, which might make problems for Internet-of-Things applications that utilization continuous information. Likewise, Internet-of-Things device tasks may not advance such a postponement.

A few investigations used Ethereum toward coordinate BC by means of Internet of Things. For example, Ethereum BC-based rich-slim customers Internet-of-Things answer for switch problems of asset-compelled Internet of Things once dealing with the excavating of BC cutting-edge Internet-of-Things uses. Moreover, lightweight stone work aimed at Internet-of-Things founded BCs that conquer the recollection cargo besides brought together problems besides simultaneously recover safety besides protection. The creators used Ethereum by way of the BC stage to ensure safety, protection besides accessibility.

5.2 Hyperledger

Hyperledger is a built-up foundation stage that remained proposed toward assistance fractious manufacturing BC progresses. It remains fundamentally a general built-up basis joint exertion including pioneers from different endeavors (around 100 people). Hyperledger remains a permissioned BC that smears admission switch, restraint cipher founded clever arrangements besides mutable understanding approaches. The permissioned Hyperledger propels and further develops safety toward evade numerous kinds of occurrences, particularly Sybil spasms. Meanwhile, the execution of keen arrangements now Hyperledger remains basically established scheduled restraint cipher execution, it gives quicker implementation between aristocracies in a couple of milliseconds. Thusly, accepting chain code shrewd arrangements gives a generous system to execute BC in Internet-of-Things applications.

Disregarding the way that there are a couple of constructions of the Hyperledger, and its Drapery is among the aimed at the maximum part ordinary besides extensively used outlines. This one is an exposed foundation besides estimated structure. A couple of thinks about think regarding the presentation of Ethereum besides Hyper-

ledger. For instance, two BC stages with testing their chance concerning the welfares besides impediments of using BC aimed at the Paris Arrangement carbon market-place instrument. In addition, a show assessment to overview the display besides limits of Ethereum and Hyperledger. Their consequences showed that Hyperledger Drapery dependably out maneuverer Ethereum to the extent torpidity, execution time, and throughput.

5.2.1 IOTA

IOTA isn't measured as unique BC stages by way of it essentially be contingent upon Jumble, additional passed on record development. IOTA can be described as a decentralized stage that supports what's more, measures various trades between passing on contraptions over the Internet. Essentially, IOTA executes an organized non-cyclic outline of exchanges rather than affixed blocks of various exchanges. This gives a few advantages, for example, it gives a lightweight arrangement as agreement doesn't need most of conveying hubs to affirm distinctive augmented exchanges, all things considered, two exchanges can be confirmed by single hubs presenting an exchange themselves. This diminishes exchange interval also above.

Light weight also a lesser amount of above structures of IOTA similarly as the usage of worked with non-cyclic outlines mark it among the maximum flexible executions of a spread data, formation of this one in a general sense a useful course of action and stage aimed at Internet-of-Things uses. Various experts exploited IOTA toward giving a useful stage for Internet-of-Things applications. The makers acquainted that IOTA tended with problems allied toward the hindrances of properties in Internet-of-Things maneuvers besides exhibited that particle shed trade charges and mining which takes colossal planning power. Then again, a couple of experts exhibited that IOTA maybe not the best response for the Internet-of-Things structure.

They induced that the computational above IOTA is in elevation, besides it is everything except a suitable plan aimed at mobile-controlled Internet-of-Things maneuvers. Table 3 gives an assessment between Ethereum, Hyperledger, moreover, IOTA.

Table 3 Examination among Ethereum, Hyperledger, and IOTA

Properties	Ethereum	Hyperledger	IOTA
Exchange time	10–15 s	0.05–100 ms	120 s
Agreement mechanism	PoW	PBFT	—
Organization usage	Less	High	Less
Calculation cost	High	Less	Less
Shrewd contracts	Yes	Yes	No

5.3 Cargo Transportation

Moving cargo is an intricate cycle including various gatherings with various needs. An IoT-powered blockchain can store the temperatures, position, appearance times, and status of transportation compartments as they move. Permanent blockchain exchanges help guarantee that everything gatherings can believe the information and make a move to move items rapidly and productively.

5.4 Segment Following and Consistence

The capacity to follow segments that go into an airplane, auto, or different items is basic for both security and administrative consistence. IoT information put away in shared blockchain records empowers all gatherings to see segment provenance all through an item's life. Imparting this data to administrative organizations, transporters, and producers is secure, simple, and financially savvy.

5.5 Log Operational Support Information

IoT gadgets track the condition of security for basic machines and their support. From motors to lifts, blockchain accommodates an alter-free record of operational information and the subsequent upkeep. Outsider fix accomplices can screen the blockchain for preventive upkeep and record their work back on the blockchain. Operational records can likewise be imparted to government substances to confirm consistence.

6 Advantages

- **Construct trust in your IoT information**—Every exchange is recorded; placed into an information block; and added to a safe, unchanging information chain that can't be changed just added to.
- **Depend on added security**—With the IoT platform you can choose the information to be overseen, broke down, tweaked, and divided between permissioned customers and accomplices.
- **Gain more prominent adaptability**—The blockchain platform is open, interoperable, and is worked for your multicloud world, utilizing the most recent form of the main Hyperledger Fabric stage, streamlined for Red Hat OpenShift.

- **Produce new efficiencies**—Blockchain smooths out measures and makes new business esteem across your environment by drawing on the information provided by IoT gadgets and sensors.

7 Blockchain IoT Stages

A couple BC stages focusing on Internet-of-thing stand developing by means of the business becomes more noteworthy. Unique BC IoT stages stand IOTA. It remained arranged expressly for IoT and gives a trade payment besides statistics move level aimed at related contraptions.

They have made the Jumble stage, which specialists depict by way of “successful past BC.” It is a block-less, cryptographic, dispersed association, wherever, as opposed to reevaluating network check, customers affirm trades of various customers.

The benefit is twofold: It thinks about more vital flexibility and it clears out the essential toward wage trade charges to diggers. Equally these issues remain basic from a typical perspective Internet-of-things system that might need the treatment of several little trades among maneuvers reliably.

Molecule has furthermore gone into a couple of critical affiliations including the following:

- **Bosch**

The Bosch XDK (Cross-Domain Development Kit) remains a programmable sensor maneuver besides Internet-of-things prototyping stage cast-off toward assemble unequivocal, steady data which would then have the option to remain vended through the IOTA Statistics Market.

- **Fujitsu**

The association remains by means of the IOTA show cutting-edge proof of thought, constant data accumulating vehicle aimed at survey tracks crossways present-day creation conditions besides source restraints.

Nest Norske Bank right now cutting-edge investigative association toward discovery habits by which IOTA’s Jumble stage can remain applied toward work on the group’s present organizations besides things.

- **Volkswagen**

The vehicle maker remains employed by means of IOTA happening an errand named “Modernized Car Pass,” which remains fundamentally an echo pass for pass set aside on an appropriated record which guarantees fundamental components—like mileage—are strong and exact.

Regardless, IOTA isn’t the solitary IoT-engrossed BC stage, others comprise.

7.1 *Hdac*

The Hyundai Digital Asset Company (Hdac) is smearing BC advancement to rapidly besides satisfactorily grant, switch character check, confirmation besides data accumulating among IoT maneuvers. The organization joins a twofold sequence structure (public, private) to extend swapping scale besides capacity, which marks it undeniably proper aimed at IoT contraptions.

The advancement is practical to wise assembling plants, splendid homes, and savvy structures aimed at machine-to-machine trades besides action among IoT contraptions.

7.2 *VeChain*

VeChain is an overall undertaking equal communal BC stage. The BC is cast-off in an arrangement of methods, through single spotlight being on state-of-the-art IoT compromise in cool chain collaborations by using prohibitive IoT contraptions to follow key estimations like temperature all through the entire outing. Besides, the stage can hold vehicle travel papers by making progressed records of vehicles including fix history, security, enlistment, and even driver direct all through its life cycle.

Clinical and clinical consideration applications are in like manner likely by means of beginning to finish following of creation patterns of clinical maneuvers and allowances of patients toward securely sharing their biometric data with their PCPs to engage progressing noticing. VeChain moreover uses IoT development for lavishness stock by embeddings shrewd chips inside the luxury things so that brands can screen their business coordinates logically, likewise thwarting unlawful over-burden trading and allowing clients the capability to affirm validness of excess thing.

7.3 *Walton-Chain*

Walton-chain is made done a mix of RFID and BC headways aimed at practical IoT joining.

They basically base onto after cycles besides things into the store organization, wherever the advancement can be applied toward best in class outfit recognizing verification, sustenance besides prescription perceptibility then collaborations following by inserting RFID names and per-user creator control chips into things. Information concerning the circumstance with things stays then downloaded for assessments on a safe BC.

7.4 Streamr

Streamr stays an open-source BC system to control the world's data economy and toward provide individuals neither switch of their individual info. Their development can remain set in interested in customary articles like vehicles to save statistics together with traffic flow, holes, and neighborhood energy costs. The customer would at that time have the option to choose, to offer this data toward singular vehicle customers or freeway workplaces. Otherwise purchase data starting various customers that resolve assistance those kind continuous choices now a related keen urban. Data goes concluded the dispersed appropriated association to become dispatched happening the association center points besides stays energized through the association's neighborhood computerized cash (DATA-COIN).

This stays impartial a little illustration of BC-based IoT stages and once over retains creating as business progresses. Various undertakings join Ambrosus, IoT Chain, Atonomi, Chain of Things, IoTeX, OriginTrail, Slock.it, BlockMesh, Helium, Moeco, FOAM, Fysical, Grid+, and Power Ledger.

8 Shortcomings with BC

- 1. BCs utilize over the top energy** Contending diggers and monster mining ranches consume a lopsided measure of power when contrasted with the result, the making of the following block. In this present reality, wherever present energy age remains an environment concern, BC preparing doesn't bode well. For what reason should Bitcoin alone utilize what might be compared to Switzerland's yearly vitality use?

There is an incongruity here. In the event that individual 1000th of the flow amount of diggers was, and accordingly 1000th of the electronic force stood burned-through, at that point Bitcoin would be similarly on par with what it is presently. It would in any case deliver one block each 10 min, measure similar amount of exchanges, then work on the very similar rapidity. The dynamism utilization for BC preparing (excavating, anyway considered besides conveyed) is a problem which does not seem prone toward vanish.

Vitality utilization ought to remain an existential problem aimed at altogether endeavors undertakings seeing BC innovation. Considerate the "power sequence" taking altogether things together his angles isn't basic. It is vital in the event that we are not to eat up the planet.

- 2. BC is definitely not an enormous appropriated processing framework** The accompanying (from now) speaks everything you may remain "underneath the feeling that BC is a type of conveyed PC," execution circulated calculations. You may have assumed that hubs across the world assemble something greater one small step at a time. That is absolutely mistaken. Indeed, the entirety of the hubs that keep a BC do the very same thing. Here is the thing that large number of PCs do

- They check similar exchanges as per similar standards and perform indistinguishable activities.
- They store precisely the similar entity into a BC (in the event that they were adequately lucky to remain permitted on the way to organize as such).
- They stock the whole past, which is something very similar aimed at every one of them, forever.

“Here is not at all resembling, no cooperative energy, and not at all shared help. There remains just moment, million crinkle replication.”

This is something contrary to effective and, while conveyed, it’s anything but a disseminated PC framework which will turnover entirely.

3 Mining doesn’t give network security Various BC (especially Bitcoin) safeguards battle that diggers keep up the adequacy besides safety of a BC. In case there remain adequate diggers this is substantial.

The issue is that miners can associate. Uncertainty they organize they hoard a coven (for Bitcoin’s circumstance, more than half of withdrawal control) they can reconsider otherwise modify the BC top. Unknown this is potential, the safety of data evaporates.

The security dispute remains that here is not at all money-related spurring power for tractors to discharge themselves into their monetary bases. This might be right wherever here is satisfactory money-related inspiration.

The counter-counter dispute is that a pernicious “performer” may imagine that its invaluable, say for political reasons, to take control, whether or not simply momentarily. The far off shot at disturbing association security should give adventures something to consider.

4 Scalability residues BC’s dimness Bitcoin is the finest BC execution based on number of customers. Anyway unbiassed 1 in each 1000 people in the world uses it. Assumed his (lethargic) trade planning rapidity, basically growing the amount of dynamic clients is not viable.

Presently think about Visa. It measures a great many exchanges each second for a huge number of clients. In spite of the fact that costly, whenever required, it can build throughput. At the point when looked at, exemplary banking (and other venture important) innovations are definitely more adaptable compared to BC.

Single attested response stays toward develop whatever is proceeding BC..

5 BC isn’t indestructible It may give off an impression of being that, expecting a BC is taken care of on every association center, remarkable organizations or experts can’t close a BC. Uncertainty not at all consolidated laborer otherwise switch opinion, here remains no spot toward drive in the direction of adjacent a BC.

Apparently this is a mental trip. Into the Bitcoin model, diggers will in everyday work in fighting lobbies. They look after this to endeavor to confirm they gain a prize aimed at their taking care of.

The test now is evading center. A BC is simply basically as abiding as this one dispersing. In the occasion that, say, over portion of diggers or workers of BC

enrolling organization be present in one nation that nation's experts can hinder in-destructibility, e.g., by removing trades or force or taking laborer farmhouses. Into the Bitcoin setting is the conspicuous risk. Yet, likenesses exist somewhere else. Business corporate take-overs may accomplish something very similar.

- 6 **Namelessness** One guaranteed fascination of BC is that it is open. Everybody approved can see everything.

On the off chance that genuine BC needs namelessness regardless of whether it adds "pseudo-secrecy" all things considered. However "pseudo-namelessness" isn't really useful for legit clients. A basic model: an organization moves an installment by means of a Bitcoin-like token. The beneficiary could possibly discover the paying organization's bank equilibrium and installment designs.

Try not to underestimate this issue. While some exposure might be worthy for (say) people, this is false for organizations. A lot of data presents perils. Abundance straightforwardness in issue monetary is a possible drawback of BC; however, it very well might be a resource in coordinations or supply chains.

- 7 **Proof of work is over the top excess** Confirmation of work is over the top excess. This is genuine regardless of whether you limit or disregard energy utilization thought.

Indeed, even evidence of stake and different arrangements utilize direct BCs. Their dependence on a lone sequence transforms into a weakness.

Here are various exercises toward evade affirmation of work. Whether or not they prevail with regard to decreasing the pointless excess measurement will require appraisal for every execution.

This is a prickly and dangerous territory, not least since understanding elective models and whether they are predominant isn't basic.

- 8 **BC can raise multifaceted design** BC development in its current status has obstacles. On the similar period, current brought together developments and organizations should change as per BC advancements, if existing hypotheses are to pass on onward.

Into this setting certain fight it looks good aimed at dares toward deliberate a cross methodology which unites groups the most awesome features of concentrated and dispersed structures. They imagine this by way of a way point scheduled the excursion to the end point of totally decentralized plan.

Issue by means of this is multifaceted design. Reason around a segment of the problems. Yield, e.g., a BC which simply grips pointers to archives detained in standard data bases otherwise possibly side chains. The BC might work with extraordinary capability and sufficiency—since it needs to quantify almost nothing. Notwithstanding, adding an outside interface, in something like one customary databases adds extra moving parts to fail.

- 9 **BCs can be there terribly incompetent** Maximum high-quality BC system customers save a complete trade past. Now the Bitcoin event, this best ever outperforms 100 GB liberal degree of the limit furthest reaches of a PC's or cell phone. More regrettable, this recreates across most, not every single, taking part node.

In the direction to save BC information, it needs to be copied. As any individ-

ual who takes at any point attempted to utilize a privately put away wallet for digital currency knows the person can't make or get installments until the whole download and confirmation measure is finished. At times this 2 or 3 days, which clients will scarcely view as progress. The option isn't to store information on each organization hub. In any case, this would

- Obliterate the establishments of distributed BCs (and look like something like conventional customer/worker).
- Expect customers to confide in workers (yet that is toward scatter "generally doubt anyone" base of BCs).

Additionally, the extra trades ready, speedier size creates. For Bitcoin's circumstance its best greater part has appeared a few ages as his omnipresence has prolonged. Here is no inspiration to feel that business BCs motivation be limitlessly unique. The Ethereum setup has gathered more than 200 GB of history statistics in the BC in his underlying more than 2 years of usage.

Clearly, a BC's future is incomplete under present conditions. In the event that a BC can't exist for "quite a while" is it worth the exertion?

9 Challenges and Issues

9.1 Slow Processing

In the BC processing major part is related to processing and remaining one is related to implementation. Because of their unpredictability and their encoded, conveyed nature, BC BCs can be moderate and unwieldy. Exchanges can require a long time to measure, absolutely contrasted with "customary" installment frameworks, for example, money or charge cards.

At the point when the client number increment on the organization, the advances take more time to measure. It can take even days to handle the entire exchange. Therefore, the exchanges cost is higher than expected, and this additionally limits more clients on the organization. In principle, the standard stretches out to BC networks which are utilized for some different option from as a store of significant worth (for instance, logging exchanges or connections in and IoT climate). This is difficult which could be fathomed with propels in designing and handling speeds, however that will take some time.

9.2 Energy and Cost

Most of BCs present in the market devour a high measure of energy. Majority of the BC innovation follow Bitcoins foundation and utilize Proof of work (PoW) as

agreement component for approving exchanges. These conventions expect clients to tackle complex numerical riddles and require huge registering capacity to check and handle exchanges and to make sure about the organization. Meanwhile, the measure of energy devoured by PCs that contend to understand the numerical riddle has arrived at an unsurpassed high. Some gauge that Bitcoin exchange energy utilization could take off as high as the yearly power use of Denmark in 2020. Add to this the energy expected to chill off the PCs, and the costs increase dramatically. To conquer this issue, numerous BC defenders are growing more proficient agreement calculations that are less energy burdening. Purported evidence-of-stake (PoS) conventions were presented that include a mix of a member's stake in the organization and a calculation to arbitrarily dole out the assignment of approval to a hub. Given that the members are not needed to comprehend complex riddles, these components fundamentally diminish energy utilization. Besides, from a business point of view, private blockchains are more appropriate to serve organization interests, as they give confined admittance, an extra layer of security to ensure proprietary innovations, and are more energy-effective.

9.3 Scalability

One significant innovation challenge of blockchain is identified with the specialized versatility of the organization which can put a strain on the selection cycle, particularly for public blockchains [2].

Inheritance exchange networks are known for their capacity to deal with a huge number of exchanges every second. Visa, for instance, is fit for handling in excess of exchanges for each second. The two biggest blockchain organizations, Bitcoin and Ethereum anyway are a long way behind with regard to exchange speeds. While the Bitcoin blockchain can deal with three to seven exchanges for each second, Ethereum can deal with around 20 exchanges in a second [2]. This absence of adaptability isn't such an issue for private blockchain networks, since the hubs in the organization are deliberately intended to handle exchanges in a climate of confided in gatherings, which bodes well business-wise.

There are some fascinating arrangements impending to handle the adaptability issue. For example, the Lightning Network, which comprises adding a second layer to the fundamental blockchain network to encourage quicker exchanges. Another intriguing arrangement is Sharding that bunches subsets of hubs into more modest organizations or "shards" which are then liable for the exchanges explicit to their shard. At the point when offered related to the evidence-of-stake agreement system can possibly scale up the application.

9.4 Interoperability

Another principle challenge is the absence of interoperability between the huge number of blockchain networks. More than 6,500 tasks [2] are utilizing an assortment of—generally independent—blockchain stages and arrangements with various conventions, coding dialects, agreement instruments, and security measures.

The issue is that with so various organizations, the blockchain space is in a “mess” because of an absence of widespread guidelines that would permit various organizations to speak with one another. The absence of such consistency across blockchain conventions additionally removes consistency from fundamental cycles like security, making mass reception a practically outlandish errand. The foundation of industry-wide norms concerning different blockchain conventions could assist ventures with working together on application improvement, approve verifications of idea, and offer blockchain arrangements just as making it simpler to incorporate with existing frameworks.

There are currently different activities that offer interoperability among various blockchain networks, for example, Ark which utilizes SmartBridges engineering to address this test and claims to give all inclusive interoperability, in addition to cross-blockchain correspondence and moves. Another model is Cosmos, which utilizes the Inter-blockchain Communication (IBC) convention to empower blockchain economies to work outside storehouses and move documents between one another.

9.5 Independent Ventures

The blockchain makes most an incentive for associations when they cooperate on zones of “shared torment or shared chance.” The issue with numerous current methodologies, however, is that they remain solitary: associations are building up their own blockchains and applications to run on top of them. In any one industry area, various chains are accordingly being created by an extensive range of associations and guidelines. This invalidates the point of appropriated records, neglects to saddle network impacts, and can be less effective than current methodologies. A positive improvements is anyway the ascent of purported blockchain consortia meant to handle industry-wide issues, including principles, minimum amount, and so forth

9.6 Integration

The real test for corporates is how to coordinate blockchain with their inheritance system(s). As a rule, in the event that they choose to utilize blockchain, associations are needed to totally rebuild their past framework, or plan an approach to effectively coordinate the two advances. One issue is that because of the absence of skilled

engineers, associations don't approach the important pool of blockchain ability to take part in this cycle. Dependence on an outside gathering can mellow this issue. However, most arrangements present available require the association to contribute a lot of time and assets to finish the progress.

Furthermore, there are the high occurrences of information misfortune and penetrate that are deterring most organizations from changing to blockchain. Each undertaking is held and reluctant to make changes to its information base, and for valid justifications, as information misfortune or information debasement establishes significant dangers. As of late, new arrangements arose which empower inheritance frameworks to interface with a blockchain backend. One such arrangement is Modex Blockchain Database, an item intended to help individuals without a foundation in innovation, access the advantages of blockchain innovation, and eliminate the perils presented by the deficiency of touchy information.

9.7 Complexity

There is additionally the absence of administrative lucidity with respect to the hidden blockchain innovation, which is a huge detour for mass reception. Guidelines have consistently battled to stay aware of advances in innovation. This is likewise the situation with blockchain. One of the difficulties of the blockchain approach (which was additionally one of its unique inspirations) is that it diminishes oversight.

Numerous associations are making blockchain innovation as a method for exchange. In any case, even now there aren't particular guidelines about it. Thus, nobody observes particular guidelines with regard to the blockchain, so there is still no security. There are sure regions that need administrative help, for example, the prior referenced brilliant agreements. In the event that the guidelines don't cover shrewd agreements, it represses appropriation just as interest in the blockchain business. Incorporated frameworks, especially in monetary administrations, likewise "go about as safeguards in the midst of emergency" in spite of their difficulties and bottlenecks. Decentralized organizations can be substantially less tough to stuns, which can affect members legitimately, except if cautious idea is given to their plan.

There is in this manner a solid contention for blockchain applications to work inside existing administrative structures not outside of them. To get over these difficulties, Government and amazingly controlled areas may need to make guidelines for blockchain. Yet, this implies that controllers in all ventures need to comprehend the innovation and its effect on the organizations and shoppers in their area.

9.8 Regulations

Awareness and understanding of any new technology will enhance its adoption and ethical use. Blockchain presents new difficulties to controllers hoping to secure cus-

tomers and markets, yet the inflexibility with which controllers on the planet's significant economies have drawn closer blockchain has served to smother development and development.

However that view is additionally changing and when likewise governments and other public associations are seeing the advantages of this innovation and build up an administrative model that supports development while securing customers that may be a stunner for other people. The principle challenge for corporates related with blockchain, particularly the little and medium ones, is an absence of consciousness of the innovation and an inescapable absence of comprehension of how it functions. Numerous organizations don't comprehend what blockchain is or what they can do. This has a great deal to do with the predominance of specialists in the blockchain territory and their excessive amount of innovation approach.

This is hampering speculation and the investigation of thoughts. Rather a considerably more business arranged methodology is a lot required. This requests improving the client experience for those not as in fact disapproved. Associations truly should instruct themselves about this arising innovation. They should expand their degree of comprehension at all levels. This requests better instructive missions to make this information more open.

9.9 Productivity Paradox

Also, there is the supposed blockchain paradox. The speed and adequacy with which blockchain organizations can execute shared exchanges comes at a high total cost, which is more noteworthy for certain kinds of blockchain than others. This shortcoming emerges in light of the fact that every hub plays out similar errands as each other hub on its own duplicate of the information trying to be the first to discover an answer.

Thusly, choices of corporates about actualizing blockchain applications should be painstakingly considered. The profits to singular preparing may reduce as the organization fills in size. This implies that blockchain applications must saddle network impacts to convey an incentive to customers or to areas on the loose.

9.10 Unavailability of Skills

While the interest for qualified blockchain staff is expanding drastically, the blockchain scene endures an intense lack of a satisfactorily prepared and gifted/qualified individuals for creating and dealing with the unpredictability of shared organizations. Blockchain innovation anyway requests extra capability and expertise. As per a few, the interest for blockchain-related positions has expanded by practically more than twice somewhere in the range of upcoming years. Having an adequate pool of qualified designers is a top industry concern.

Blockchain innovation is as yet in its earliest stages is as yet developing. It requires time for the engineer network to receive it, and for instructive foundations to present applicable blockchain-related courses. In spite of the fact that this will mitigate the market interest, the outcomes anyway will get unmistakable simply after understudies will complete their preparation and that will take some time.

9.11 Reputation

Reputation [1] is a worldwide impression of an element's conduct in light of the trust that different elements have set up. Reputation frameworks have various objectives, including picking dependable assets, ensuring honest behavior of nodes, and quality of the content of a mutual record. Reputation frameworks need to battle with the referred to issues, for example, how to keep reputation information exceptional, precise, and circulated to a wide arrangement of users which changes progressively, are confronted when conveying such standing framework. In blockchain, it is difficult to keep reputation intact. Bad mouthing, Collusion, Sybil, and re-entering attack are handled in blockchain up to a level but not completely. Blockchain is utilized for logging hub activity, permitting any single node to compute the standing of guaranteed hub to recognize and dispose of nodes that will in general abuse assets of the entire bunch and don't contribute by their calculation assets or contribute by bogus outcomes.

9.12 Security and Protection Challenges

Furthermore, what to think about the different security and protection challenges. While digital forms of money offer pseudonymity, numerous likely utilizations of the blockchain require shrewd exchanges and agreements to be unquestionably connected to known characters, and subsequently bring up significant issues about protection and of the security of the information put away and available on the mutual record. Numerous organizations these days work with protection rules administered by guideline. Their shoppers trust them with delicate data. In any case, if this data is totally put away in a public record it won't really be private any longer. Private or consortia blockchain could work here. You would get restricted admittance, and all your touchy data would remain private as it should.

Security is another essential theme here. Nonetheless, just a small bunch of situations have great conventions that can adapt to this. While blockchains are safer than conventional PC frameworks, programmers can in any case break applications, frameworks, and organizations based on blockchains. The arrangement isn't simply government insurance of security. Self-sovereign personalities on blockchain will empower us to catch and control our own information. While there is a ton of work

on a few protection conventions, for example, verification of zero information to defeat these deterrents and great personality activities are in progress (Sovrin), we are as yet far from a profoundly new character structure.

10 Ongoing Projects

IoT and blockchain are cooperating as one to improve the world an associated place. Instances of IoT and blockchain remember everything from record security for modern IoT hardware to blockchain being utilized as a technique to track-and-follow IoT-empowered steel trailers.

The following are eight instances of how Internet-of-Things organizations are utilizing blockchain to improve the world an associated place.

10.1 HELIUM

Helium is the world's initially dispersed machine organization. The organization utilizes BC to interface low-power IoT machineries (like switches and CPUs) to the Internet. Helium's BC-based isolated network groundwork utilizes wireless innovation to reinforce web association and fundamentally diminish the force expected to run "savvy" apparatuses.

The Helium group as of late did their first fruitful blockchain exchange, and the organization currently plans to execute their hubs across California, Boston, and the UK to test their distributed decentralized organizations.

10.2 Chronicled

Chronicled joins blockchain and IoT items to convey a start to finish inventory network arrangement. Zeroing in on the drug and food supply businesses, Chronicled utilizes IoT-empowered steel trailers and sensors to give continuous updates on delivery measures.

Executing blockchain in their IoT gadgets takes into account all gatherings engaged with a medication or food supply transporting interaction to be completely mindful of the chain of care and if any issues emerge during the cycle.

Chronicled as of late built up a specialized pilot showing how production network occasions can be enrolled on a blockchain. The blockchain considered the drug business' severe information security strategies and convoluted taking care of rules to effectively record a production network of occasions.

10.3 ArcTouch

ArcTouch makes in addition to construct BC-based software design for a possibility of savvy, related things, comprising voice collaborators, wearables, and shrewd TVs. The organization takes constructed modified, dispersed applications DApps for numerous administrations that attach to IoT devices. DApps of ArcTouch give an additional grade of IoT safety and can deal with arrangements faster concluded savvy contracts. The association has accumulated a uncommon BC DApps that interface with IoT devices like Amazon, Alexa, and Facebook Messenger.

10.4 Fiber

Filament plans blockchain-upheld equipment and programming that effectively incorporates with IoT items. The organization's blockchain suite, called Blocklet, centers around fortifying information security in IoT gadgets for the development, assembling, energy, and transportation ventures.

Fiber's DLT environment gives a supported network protection convention and takes into consideration speedier correspondence between IoT gadgets in enterprises that need it most.

Filament as of late made the Blocklet USB Enclave, an industry first. The blockchain gadget connects to any USB port and can promptly dispatch any tasks on a blockchain.

The organization likewise has a Blocklet central processor underway that can be incorporated into an IoT equipment framework.

10.5 NetObjex

NetObjex has made a normalized, decentralized instrument for IoT gadgets to speak with each other. The organization's blockchain-empowered IoToken gives a protected advanced stage to smart gadgets in a similar biological system to cooperate and impart.

NetObjex claims its IoToken can be utilized to consistently speak with different gadgets in a heap of enterprises. At a drive-through café, supporters could utilize the IoToken in their crypto wallet to pay for their supper. In drone conveyance, the IoToken can be utilized to stamp a state of conveyance and confirm installment.

The organization banded together with the Brooklyn Public Library to introduce its Smart Mobile Phone Charging Station innovation. Controlled on NetObjex's blockchain-IoT innovation, the charging stations expect clients to watch a concise enlightening video and take a short review.

The aftereffects of the overview are safely put away on a blockchain for the Brooklyn Public Library to break down as a feature of its developing activity to improve benefactor experience.

10.6 HYPR

HYPR utilizes decentralized organizations to get associated ATMs, vehicles, bolts, and households. Some of the primary explanations cyberattacks are consequently decimating and far reaching are that concentrated information bases stock a great many keywords.

HYPR stocks biometric logins taking place their BC, getting and distributing significant statistics. The administration's biometric safety pacts incorporate special facial, eye, voice, and palm acknowledgment apparatuses for IoT devices.

HYPR has effectively explored different avenues regarding a few diverse decentralized uses for their IoT security stage. They have tried biometric checks on cell phones to get to ATM individual banking, and the organization made a DLT computerized key for mortgage holders to have a solitary passage to everything from IoT-empowered ways to savvy amusement focuses.

10.7 Xage Security

Xage is the first blockchain-ensured security stage for IoT. Zeroing in on mechanical ventures like farming, energy, transportation, and utilities, Xage's blockchain empowers IoT gadgets to be sealed and approaches secure lines of correspondence between shrewd items.

Xage has a setup of decentralized IoT applications that do everything from safely overseeing strategy to offering devices that issue moment alarms about dubious hacking action.

Xage as of late joined the Smart Electric Power Alliance (SEPA) to zero in on how it can carry its IoT gadgets to the spotless energy area. The organization needs to make its record innovation more far reaching to ruin digital assaults.

10.8 Grid+

Grid+ utilizes the Ethereum blockchain to give purchasers admittance to energy-saving IoT gadgets. An organization specialist purchases and sells power for a Grid+ client, the Grid+ application helps offer state-of-the-art data about energy use and the organization's brilliant meter remotely interfaces with energy-saving savvy gadgets.

The organization's Ethereum blockchain empowers specialists to pay for an effective measure of power like clockwork. Installments and network protection on the application are executed utilizing progressed blockchain cryptography.

As the world's first blockchain-based energy retailer, Grid+ as of late presented the main model of its representative, Lattice1. Utilizing Ethereum, Lattice1 can recognize variances in the energy showcase and decide the most proficient value point continuously. The home improvement shops digital forms of money and will utilize these for energy installments.

11 Future Research Directions

Forthcoming Research Ways of IoT with BC Notwithstanding the blend of IoT with BC takes a couple of benefits that one in like manner carries various problems that stand decided to get the complete reimbursements of the two developments. This part gives a conversation of upcoming investigation headings of IoT with BC development.

11.1 Security

The IoT organization incorporates several of assorted IoT things that be there arranged with slight safety in prospect of their creates. These contraptions with deprived fundamental safety processes remain a direct engraving for numerous safety aggressors. Regardless of the way that getting IoT together with blockchain development can further develop the IoT security by utilizing encryption, constant nature, painstakingly planned, and progressed mark structures of BC advancement, the safety is at this point unique defies in doing a capable what's more, practical IoT structure with BC.

Through the growing choice of IoT maneuvers and uses, here is an extending bearing in the direction of broadening the usage of distant associations, particularly in mechanical spaces. Though far off correspondence gives a couple of advantages, it moreover encounters a couple of safety shortcomings like replaying attacks, inactive snooping, and staying. Moreover, on account of the restrictions of properties in IoT maneuvers, refined and cutting-edge encryption computations can't be exploited in IoT structure. Then, at that point, blockchain advancement has its safety inadequacies. For example, here are software package forsakes of smart agreements and dispersed self-ruling association attack. Subsequently, here is a requirement for additional investigation to explore safety matters in IoT and BC.

11.2 Flexibility

Among the focal inquiries of joining blockchain through IoT is limit of the BC to measure what's more, exertion successfully using a colossal degree network similar to IoT. The input of trades each sec can remain cast-off to check flexibility of BC contrary to the amount of IoT maneuvers. BC stages give defenseless amount. For example, Bitcoin can simply manage seven trades for consistently. Furthermore, Ethereum can simply deal with 20 trades each sec. Alternately, VISA can quantify very approximately 2k trades each sec and PayPal has an output of 170 trades each sec.

Appropriately, this planning speediness can't statement the solicitations of IoT which comprises several trades. Also, a couple of IoT uses are mostly operational by way of progressing data, through confined throughput of BC, and therefore these uses will defy intricacies altogether work gainfully.

Disregarding the way that there are a couple of proposed answers for resolving the adaptability issue of blockchain development like construction more flexible arrangement estimations and arranging private BC meant for IoT, here is a prerequisite for additional assessment in the direction of track down a powerful response for this issue.

11.3 Data Storage

Blockchain isn't worked to record huge volumes of information. Interestingly, the IoT framework is deliberated as per unique of the wellsprings of large information. The volume limit is among the significant issues of blockchain innovation.

The dimension of the whole Bitcoin BC is about 150 GB, additionally, the dimension of the whole Ethereum BC is about 400 GB. Putting away altogether squares of the BC is required. Devoid of taking every single past block, IoT gadgets can't approve the exchanges delivered by different gadgets. Also, authentic information are needed to deliver new exchanges. Thus, all information made through IoT gadgets, which be present in ZB, should remain put away on BC, which isn't possible. Furthermore, the expense of putting away information on the blockchain is pricey. For example, the expense of putting away 1 GB of information is about 2000000\$ in Ethereum. This cost isn't down to earth for different IoT applications and administrations. For sure, the union of IoT using BC eliminates need for a unified worker to retain IoT information, be that as it may, information stockpiling in the BC is actual troublesome besides costly. Henceforth, here is a requirement for additional exploration in research novel techniques to determine this concern.

11.4 Legal Issues

Every novel innovation like IoT and BC is influenced through guideline and rules of every country. Amid the problems that hold up traffic of coordinating IoT and blockchain effectively is the absence of laws, particularly with respect to blockchain. Since blockchain gives obscurity highlights, it is troublesome to recognize the genuine personalities of their clients, making it a reasonable climate for crooks. Hence, various nations actually have a few problems nearly in what way to manage BC innovation and how reasonable regulations and guidelines that is utilized to regulator another climate.

Similarly, IoT gadgets gather a colossal measure of information about their proprietors. This data can incorporate delicate and classified information. Utmost IoT gadgets use this data with their produces or else specialist organizations devoid of taking approval commencing their proprietors. This totally abuses the protection of gadgets' proprietors.

11.5 Restricted Resources

Most IoT gadgets have restricted assets as far as memory, preparing force, and energy. For example, smart meters make sure to work on low battery-operated energy, restricted capacity, and small figuring. Incorporating such asset-compelled IoT gadgets with blockchain innovation will confront a few issues. For example, agreement instruments need thorough handling control and burn-through concentrated energy. Thus, agreement systems with tremendous handling and force requests can't work with IoT gadgets with restricted assets. Besides, as examined prior, the capacity limit is amid the significant problems of BC, as per the all-out dimension of Bitcoin and Ethereum BCs are about 150–400 GB individually. Be that as it may, IoT gadgets produce information in ZB. Accordingly, BC is not appropriate meant for putting away IoT information.

Potential answers for this issue might be incorporating distributed calculating with IoT in addition with BC to solve problems of the asset requirements of IoT entities. The primary concern determines by which to coordinate incorporated distributed computing with BC to give proficient resultant innovation.

12 Conclusion

Blockchain is another innovation, regularly alluded to as the Internet of Value. Likewise with every new innovation, there is no agreement on its expected worth, with certain individuals guaranteeing that it will bring more troublesome changes than the Internet and others challenging the degree of its significance. Notwithstanding

forecasts that what's to come is risky, there is proof that blockchain is a noteworthy, new innovation that will change the manner in which exchanges are made, in light of its capacity to ensure trust among obscure entertainers, guarantee the changelessness of records, while additionally making delegates old. Organizations are zeroing in on usage of blockchain with their administrations to guarantee security and unwavering quality. Still they are confronting difficulties and issues for improvement and usage of blockchain-based administrations.

Blockchain should defeat various issues before its full favorable circumstances can be misused, however so was the Internet before October 1990, when Sir Tim Berners-Lee presented three crucial advancements that shaped the establishment of the World Wide Web (WWW) and are used until the present time. Before the finish of 1990, the principal site page was posted on the web, which individuals could visit and view data on, generally communicated through modems and standard phone lines. Notwithstanding, such data comprised of text just characters, as sounds, pictures, and recordings were outside the correspondence capacities of that time. Google, Amazon, Facebook, or YouTube was impossible around then, when in any event, sending an email, before the Mosaic Internet browser was presented, was viewed as an innovative accomplishment. No one should be amazed; hence, with blockchain's present constraints, all things considered at around a similar stage as the Internet was during the 1990s.

In this chapter, the center favorable circumstances of blockchain and brought up that its maximum capacity what could be compared to Google, Amazon, and Facebook, arising to abuse the upsides of blockchain advancements. This chapter emphasizes the estimation of blockchain and its troublesome nature while too thinking about its future accomplishments. A Deloitte Global Blockchain Survey closed that 2019 was a defining moment for blockchain when an extreme move occurred in the mentalities of business pioneers who perceived that blockchain is without a doubt and that it can fill in as an even minded answer for business issues across ventures and use cases. That is, these pioneers perceived a move from "blockchain the travel industry" and investigation toward the structure of reasonable business applications, as blockchain has at long last entered the standard of business applications. Blockchain ensures trust, guarantees permanence/straightforwardness, and supports disintermediation notwithstanding giving extra security for exchanges executed over the Internet. These are extensive points of interest that can't be overlooked, while its detriment of the expense of execution can be devalued and decreased in a short measure of time, as more involvement in applications is picked up and blockchain turns into a center innovation. In particular, in any case, as use expands the inspiration for upgrades will increment, as well, as has been the situation with the Internet that saw considerable headways over a brief timeframe. Such headways will give answers for blockchain's failure to scale, fundamentally lessening utilization costs.

The eventual fate of blockchain will move in two unmistakable ways. The main will incorporate every one of those applications requiring decentralized, super made sure about organizations as those examined previously. IoT, AVs, BCI, and BBI will be remembered for this classification as will shrewd agreements and DAOs. There will be no decision except for to utilize blockchain in these applications. The

other heading will remember progresses for AI that when joined with blockchain can significantly improve its worth. Such advances will incorporate improving the well-being of huge information just as its capacity to decentralize who holds it, as of now only claimed by organizations like Google and Facebook, and democratize proprietorship and sharing by making a commercial center where such information can be exchanged. This will imply that people can keep control of their information and choose their own when and how to make it accessible to outsiders. Also, more modest Artificial intelligence players will have the option to use this information and further development of AI notwithstanding the enormous firms, hence breaking their information restraining infrastructure. Another region where blockchain and AI can coordinate is in online protection, by joining AI and blockchain together to make a twofold shield against cyberattacks via preparing ML calculations to mechanize constant danger recognition and to persistently find out about the conduct of aggressors, while decentralized blockchains can limit the characteristic weakness of unified information bases.

Blockchain's capacity toward security and unchanging nature can likewise be utilized for putting away the exceptionally delicate, individual information expected to decide designs in touchy cases, for example, those including the medical services area. Besides, blockchain can add to breaking the black box of AI by following how calculations work and how their info influences the yield of AI, while AI can increment the effectiveness of blockchain much better than people, or standard figuring. At last, Bitcoin, seen as blockchain's first inventive achievement, can add to applying the innovation to extra zones, expanding the prevalence of both Bitcoin and AI, just as their different applications. Blockchain and Simulated Intelligence are new innovations and much will rely upon future, yet obscure, mechanical progressions. Nonetheless, there is impressive potential that can raise their different, just as their joined, helpfulness to new, significant levels of significant worth and appropriateness. This has been the situation with the Internet as well as all new advances whose future worth has been belittled significantly at the beginning.

Acknowledgements This work was sponsored by SERB, the service of the Department of Science and Technology (DST), Government of India, Project “SWARD—Secure next-generation Wireless Access RaDiO technology for smart cities in India” (award number EEQ/2018/001482).

References

1. Bellini E, Iraqi Y, Damiani E (2020) Blockchain-based distributed trust and reputation management systems: a survey. *IEEE Access* 8:21127–21151
2. Meijer CR (2020) Remaining challenges of blockchain adoption and possible solutions
3. Tseng L et al (2020) Blockchain-based database in an IoT environment: challenges, opportunities, and analysis. *Clust Comput* 23(3):2151–2165
4. Mohanta BK et al. (2020) Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology. *Intern Things* 100227
5. Mistry I et al (2020) Blockchain for 5G-enabled IoT for industrial automation: a systematic review, solutions, and challenges. *Mech Syst Signal Process* 135:106382

6. Hakak S et al (2020) Securing smart cities through blockchain technology: architecture, requirements, and challenges. *IEEE Netw* 34(1):8–14
7. Torky M, Hassanein AE (2020) Integrating blockchain and the internet of things in precision agriculture: analysis, opportunities, and challenges. *Comput Electron Agricul* 105:476
8. Bhushan B et al. (2020) Unification of blockchain and internet of things (BIoT): requirements, working model, challenges and future directions. *Wireless Netw* 1–36
9. Alanazi M, Soh B (2020) Blockchain-based framework for enhancing IoT security. *J Xi'an Univ Architect Technol* (2020)
10. Singh S et al (2020) Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustain Cities Soc* 63:102364
11. Zehir S, Zehir M (2020) Internet of things in blockchain ecosystem from organizational and business management perspectives. *Digital business strategies in blockchain ecosystems*. Springer, Cham, pp 47–62
12. Farahani B, Firouzi F, Luecking M (2021) The convergence of IoT and distributed ledger technologies (DLT): opportunities, challenges, and solutions. *J Netw Comput Appl* 177:102936

Blockchain for IoT-Based Cyber-Physical Systems (CPS): Applications and Challenges



Reham Abdelrazek Ali, Elmoustafa Sayed Ali, Rania A. Mokhtar, and Rashid A. Saeed

Abstract Cyber-Physical System (CPS) enables to combine the physical objects with computing and storage capabilities to have data exchange in an interconnected network of systems and objects. Blockchain is a recently distributed computing paradigm that provides a promising solution for modern CPS application. It forms an underpinning technique for CPS that offers strong added value to industrial IoT (IIoT), fault-tolerant, reliable, secure, and efficient computing infrastructure. The inherent integration of consensus algorithms and distributed storage with advanced security protocols provides powerful solutions for CPS applications. Blockchains in CPSs/IoT ensure secure and saved information for different industrial applications and achieve a means of adaptability, process, and operation protection, for example, in manufacturing, transportation, health care, and energy applications. This chapter will provide extensive technical background for blockchain in IoT-based CPS. Applications, opportunities, and challenges for the combination of CPS, IoT, and blockchain were presented.

Keywords Blockchain · IoT · IIoT · Cyber-physical system · Distributed applications · Privacy · CPS · Cyber systems of system

R. A. Ali · E. S. Ali (✉) · R. A. Mokhtar · R. A. Saeed

Department of Electronics Engineering, Sudan University of Science and Technology,
Khartoum, Sudan

E. S. Ali

Department of Electrical and Electronics Engineering, Red Sea University, Port Sudan, Sudan

R. A. Mokhtar · R. A. Saeed

Department of Computer Engineering, Taif University, Al-Taif,
Kingdom of Saudi Arabia

1 Introduction

The misuse of blockchain within the domain of IoT, cyber-physical system (CPS), and future Information and Communication Technology (ICT) foundation in common has the potential to empower different capabilities and use-cases in those frameworks. From a security viewpoint, blockchain innovation can set up conveyed security in different to centralized designs [1]. Within the moment put, blockchain's solid assurance against information altering makes a difference to avoid a rebel gadget from disturbing communications including domestic, production line, or transportation frameworks by infusing or transferring malignant data. Additionally, since blockchain is built for decentralized control, different checking and choice plans based on blockchains ought to be more versatile than customary ones [1, 2]. Later progresses in electronic and remote communication have changed the IoT through the advancement of scaled-down gadgets that can utilize and oversee the collection and trade of information. These focal points have empowered the advancement of little, cost-effective, and more controlled multi-functional detecting stages competent for checking and communicating different data in different segments, such as vehicular, health care, industry, and numerous more [3].

The IoT approach is presently combined with inventive calculation to extricate a bit of profitable data that can be valuable by other physical gadgets making a CPS. The CPS comprises of physical portion and cyber-part associated through a communication organize. This framework is profoundly significant to the industry and other areas like restorative and health care. CPS is presently being connected through an assortment of businesses; Blockchain has got tremendous attention as it implies to supply security, secrecy, auditability, and belief. Be that as it may, the existing blockchain-based arrangements endure some challenges and in this way are not specifically pertinent in CPS [4].

Because of recent research interests on the importance of blockchain in CPS and IoT applications, this chapter provides a brief concept about blockchain use in IoT-based CPS systems. The chapter is organized as follows; Sect. 2 presents the revolution of CPS in addition to brief history. In Sect. 3, the chapter reviews the idea of CPS multi-paradigm modeling and characterizations. In Sect. 4, the chapter provides a methodology of designing the CPS base on the system of systems and the use of CPS in IoT in Sect. 5. Moreover, the chapter also reviews the blockchain use in CPS and the framework of blockchain in IoT/CPS in Sects. 6 and 7, respectively. In Sect. 8, the chapter provides different applications related to blockchain IoT-based CPS. The challenges of blockchain IoT integration to CPS are reviewed in Sect. 9, in addition to the effective adoptions' barriers of blockchain IoT-based CPS in Sect. 10. Finally, chapter conclusion is given in Sect. 11.

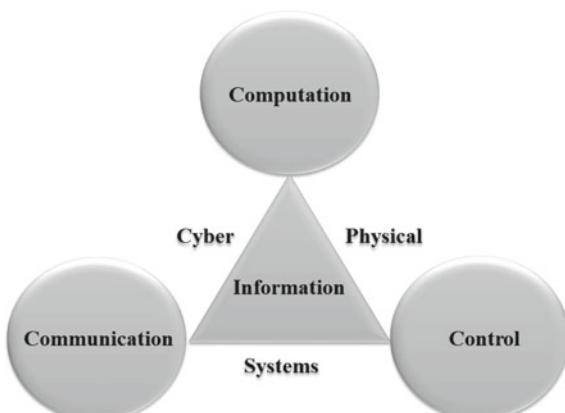
2 The Cyber-Physical Systems Revolution

In 2006, the US National Science Foundation released the cyber-physical systems as a new vision for how to fully computerize and engineer the hardware and physical components in an integrated way [5]. Where the process of integrating computing with physical systems is defined by what is known as a cyber-physical system (CPS) [6]. CPS integrates dynamic physical processes with computing and networking systems to help integrate systems, design, and analysis used in intelligent industrial process applications. Inserted computers screen and control physical forms, as a rule with criticism circles, where physical forms influence computations and bad habits versa. CPS helps to combine the computing systems applications with the strategies for building models for systems of a mechanical and electrical nature, as well as chemical and biological processes [7].

CPS goes beyond traditional presentation to dynamic framework models to understand physical effects across the physical cyber interface via sensors that link information between physical and electronic parts [8]. In other words, CPS is a basic system that works to link the physical parts in industrial applications with the cyber world. The plan of CPS is right now a driver for development over different businesses, making unused markets [7, 8]. More proficient CPS will affect positively in financial issues related to industrial applications. CPS is related to the innovations empowering computerized assets and physical objects to have interacted with each other in ways to handle numerous provide assignments.

CPS combines the physical, biological, engineering, and information technologies parts based on software and computing as shown in Fig. 1. As an example, the concept of CPS technology has been used before by Germany during the second War to monitor the wings of military aircraft [9]. In the CPS system, it's important to ensure that embedded systems can provide real-time processing for critical applications. According to this concept, many industrial systems were built using CPS

Fig. 1 Cyber-physical system



technology and revolutionized the field of industrial computing. With the communications revolution and IoT technologies, it has become possible to integrate physical electronic systems with the Internet of things as a frame of CPS/IoT to provide advanced models for modern industries [10].

3 Multi-paradigm Modeling of Cyber-Physical Systems

Multi-model modeling (MPM) is defined as a method that enables the ability to adapt the planning and communication of CPS to modeling several intelligent disciplines. MPM provides an understanding of the modeling of each part of complex systems on several levels, using the appropriate model for each complex engineering work [11]. About CPS, MPM helps to develop an effective design model. The concept of Multi-Model Modeling (MPM) appeared in 1996 to establish the rules of reanalysis by a multi-model methodology using a combination of different abstract representations [12].

MPM provides flexible identification of a wide range of distinct topics, providing tools that can shift from theoretical to application-oriented methods. In cyber systems, the physical component can be controlled by several smart methodologies that help to allow the physical parts to interact with the desired objectives [13, 14]. Concerning the CPS model, each atomic CPS is linked with one physical component, so that it represents the mechanical behavior, in addition to linking with an electronic component that regulates the computational function of the physical component. As can be seen in Fig. 2, the atomic CPS does not contain any subsystems but has a special element that defines its function. In CPS, the cyber and physical component classes are considered as a subclass of the CPS general class component that characterizes the common properties of these classes. Also, these classes can communicate with any other component through their I/O interfaces.

In the control framework, the controller part enables control of the acts in the physical environment component by any implies of control activity, in addition, to recognize the current value of variables within the physical component [15]. The controller at that point makes a sequence of control activities to rectify and act as a control framework. It helps to recognize a control framework from a CPS [16]. In general, there is no single characteristic that distinguishes CPS, so it is found that physical cyber frameworks contain a large number of link parts and have several characteristics, where these characteristics are linked to several issues such as [17].

- A. **Large-Scale Physical Electronics:** CPS is concerned with the operation and logic of controlling these components, which contain several cyber sub-components that deal with a large number of original data.
- B. **Huge Operations Scale:** CPS enables to outreach a few millions of components and complexity intuitive.

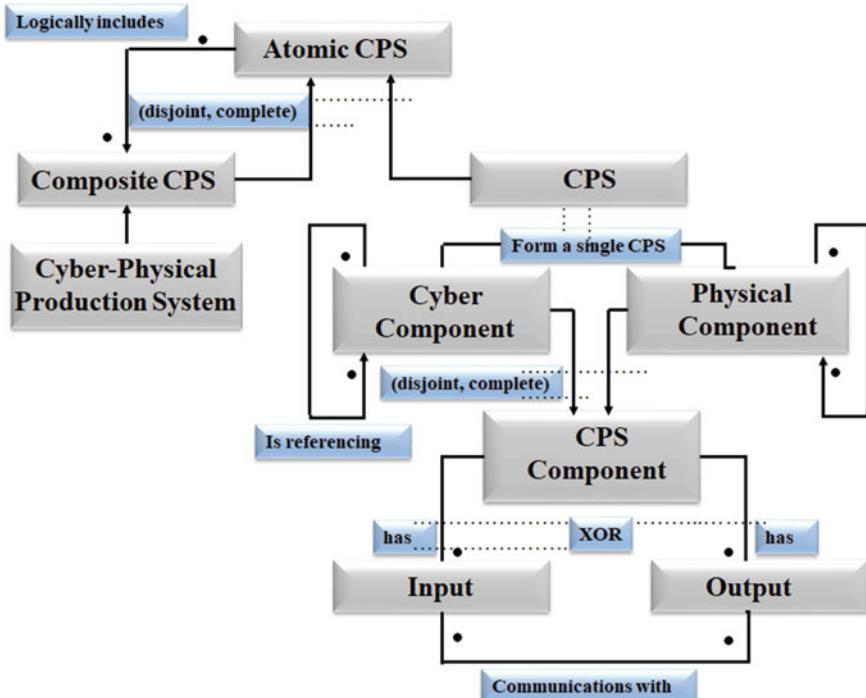


Fig. 2 Multi-paradigm meta-model of CPS

- C. **Discrete hybrid Nature:** This is defined as the association of many separate electronic and hardware parts in the form of a cross framework. Many of these parts are very heterogeneous according to their types.
- D. **Integration with Numerous Outside Frameworks:** its ability of handling information and occasions in particular designs from different frameworks with changing transfer speed and message conveyance guarantees.
- E. **Heterogeneous Interface:** Highly organized and progressive interfacing of numerous components regularly through computerized systems with efficient communication buses and protocols.
- F. **Adaptability:** CPS is adaptable as the framework must change its behavior to designs that may not be computed for a specified plan time.

CPS moreover builds on implanted frameworks, which are stand-alone frameworks that integrate components of control logic and interaction in the real world. An inserted framework is regularly a single gadget, whereas CPS incorporates numerous constituent frameworks. Encourage, implanted frameworks are particularly outlined to attain a constrained number of assignments, regularly with constrained assets [18]. A CPS, in differentiate, works at a much bigger scale, possibly counting numerous inserted frameworks or other CPS components counting human and socio-technical frameworks [19, 20].

4 Design of CPS Based on System of Systems (CPSoS)

CPSoS is a large-scale complex framework that is connected to hardware and controlled using several computing mechanisms, as well as human clients [21]. The system of systems (SoS) concept lies within the possibility of integrating several interoperable frameworks so that they are organized to work together at a time to achieve a specific goal [22]. These kinds of frameworks need a modeling strategy with specific details and modeling able to describe the frameworks of SoS within the cyber-physical key characteristics like (a) operational freedom of the components of the by and large framework, (b) managerial autonomy of the components of the general system, (c) geographical dispersion and Developing behavior, and (d) evolutionary improvement processes [23].

Complex CPSs depend heightening on the trade of modest bunches of individual physical, communication, and computing systems. The proposed plan strategy for CPS frameworks is based on the system of system approach as appeared in Fig. 3. In the cyber-physical system of system framework, the prerequisites for cyber-physical frameworks are referred to as characteristics of platform-specific frameworks that are depicted using the capabilities of the system-wide core component frameworks according to specified criteria [23, 24].

In CPS Frameworks of Frameworks (CPSoS), there are some requirements for unused necessities building forms, administration strategies, methods, and apparatuses that can powerfully react to unsteady, divided, ceaselessly changing necessities. The CPSoS strategies and apparatuses ought to not only be able to bargain with issues that are related to impact necessities, cascades impact, scourges but also it must be able to handle issues related to apportioning a large-scale framework of frameworks into different independent autonomously advancing constituent frameworks. CPSoSs are cyber-physical frameworks that display the highlights of frameworks as follows [24]. The possibility to dynamically configure the outline on various time scales. The regularly spatially transmitted large physical frameworks with complex elements. And the ability to distribute, control, supervise, and manage, with an ability of partial independence of the subsystems.

Some of the important issues and challenges related to CPSoS tools and methodologies related to the collaborative environments of competing firms, the process of integrating legacy systems with the model-based engineering requirements of the whole system's life cycle [25]. In addition to other issues such as related to exploring the design space while considering heterogeneity, control, and validation of CPSoSs, also analyzing how the type of hierarchical, decentralized, and distributed control affects performance and its relevance to the new custom algorithms for controlling and validating CPSoSs. There are also other challenges such as modeling issues and CPSoS simulation such as multiple scales, human interaction, and fault management [22].

In CPSoS, multiple scales can be combined into subsystem models, which can add a degree of potential for model development and integration. In addition, it is possible to blend human interaction with systems by using behavioral patterns that express the

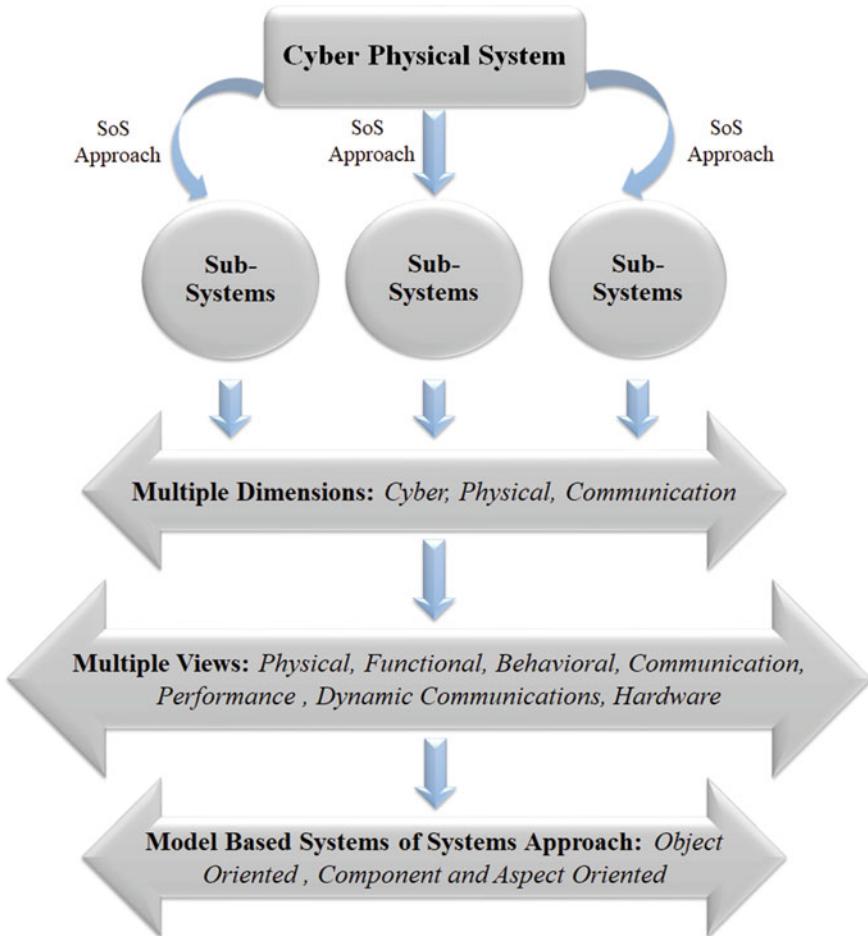


Fig. 3 Methodology for cyber-physical system of systems approach

nature of human behavior. The CPSoS also enables to perform the fault management in case of any subsystem degrading conditions related to dynamic reconfiguring in CPSoS, and issues in heterogeneous data integration and synchronization as well [25].

In CPSoS, modeling and simulation provide vital improvement to design and operate such systems, in addition to facilitate the ability to design complex systems models in reliable and sufficient significantly [22]. There are some challenges in designing a CPSoS module, which is the high cost of building and maintaining the modules. Also, reusing the designed models and investigating their random behavior is considered one of the challenges that need fundamental consistency in the theoretical and design aspect [24]. These challenges fall within the domain of large-scale re-representation of heterogeneous frames, re-representation of

productive hybridization, as well as the re-representation of frames with many diverse timescales. Add to this, the coordination of re-enactment of the physical part of the framework and management methodologies to achieve implementation that accounts for anomalies [26]. Hence, due to its scaling and complexity relative to real timeframes, complex CPS frameworks show various formative challenges. The long-term reasonability of complex cyber-physical frameworks goes up against these challenges through the advancement of unused detail, modeling, plan, composition, confirmation, and verification approaches.

5 Cyber-Physical System Architecture for IoT

The design of CPS/IoT is an important process for planning and developing the architecture of CPS systems that rely on access to the Internet, so that the mechanisms related to control and computing are identified, in addition to archive the capabilities to carry out relevant approaches for the operation of cyber systems on the Internet. In designing CPS/IoT framework, the modeling should be taking the considerations of progression and depiction of layers independently that seek after the components and duties of non-specific layered engineering, as we know IoT incorporates the objects or things that utilize web network. [27]. Several IoT architectures can be applied to build services for smart infrastructures. Figure 4 shows a simple IoT architecture used for CPS.

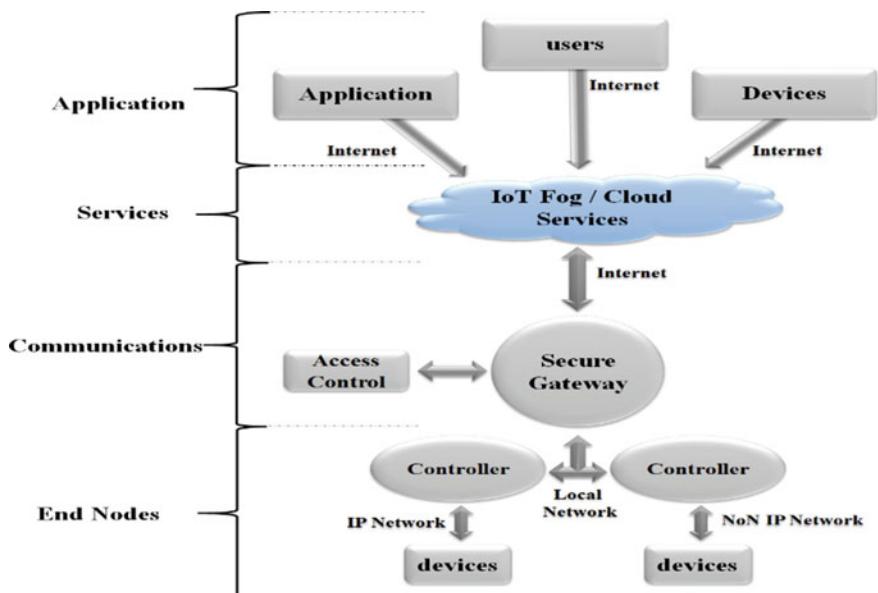


Fig. 4 CPS-based IoT hierarchy simple architecture

CPS IoT-based architecture is considered as a network that consists of a finite number of processes, tools, schemes, and systems those able be connected through the internet to provide many services and exchange data between physical systems and humans. On the simplest examples for IoT systems, those may be acting with CPS like GPS systems, smart mobile devices, and transport systems [28]. The description of CPS/IoT layers architecture can be summarized according to the following tasks [29].

- A. **Communication and Connectivity:** CPS/IoT can use different web conventions. The IoT layer also enables the communication between tools and gives a link that is generally centered at the network edge.
- B. **Preprocessing and Analytics:** when information is gotten from the primary layer, it continues to the following explanatory portion for change in computerized shape, which machines can effortlessly able to preprocess essential data. Fundamentally, this preprocessing and analytics layer is dependable for dispersing information over wired/remote doors whereas empowering peer-to-peer connect. After that, information preprocessing, information accumulation, the transformation of information from analog to advanced, information component examination, and distributed analytics ended up the most obligation of this layer concerning the system's need.
- C. **Management and Visions:** This layer works for administration and insights enables to make the administration of related tools by taking care of choice-making about notices, uploading, downloading, overhauling applications, in addition to ceasing and rebooting tools. Moreover, it enables dealing with errors, caution settling, and oversees the central communication inside the endpoint devices.
- D. **Control Operations:** This layer is a fourth-order control layer that serves to arrange, create, and oversee the planning, creation, and oversight of the Application Program Interface (API). This layer is one of the most important layers because it works on early guidance for changing administrative tasks to control tasks.
- E. **Applications:** This layer transfers the result from the control stage to the state of preparing the result through the use of smart applications, special mechanical applications, websites, and multi-use applications. It also offers the processes for making calls to APIs, etc.
- F. **Business Aspects:** This layer includes customers, partners, and business owners as a major part of the system, in that it defines the cooperation of forms and people by developing primarily in the market.

6 Blockchain-Enabled Cyber-Physical Systems

CPSs are an engineering worldview associated with unavoidable detecting and communications advances to supply different advantages to the society and economy. In different words, built framework in which the electronic circuit structure or preparation is increased with the soft component, such as processing equipment and

communications chips [30]. The component is exceptionally firmly coordinating among selves, which cruel the usefulness of one function is subordinate on other components. CPSs have seen great development in later a long time in ranges, such as vitality, well-being, transportation, and the Mechanical Internet of Things (IIoT) blockchain, a dispersed framework to oversee exchanges, which employments organize members to construct belief, is being considered as a reasonable elective to secure against cyber-attacks [31]. Such dispersed frameworks have numerous points of interest as related to central frameworks, which fall flat to measure as the associated client's increments number.

Blockchains are unchanging conveyed databases to which current time stamp exchanges could be added and gathered into sequence blocks chains [32]. The fundamental of blockchains convention characterizes appear numerous duplicates of such squares can be built and kept up in a conveyed design. The main viewpoint of these conventions is choosing how an organization of members, identified as miners, can set up agreement blockchain present status. These processes accept that, for all system times, as it were a division of the diggers may turn malevolent or flawed. There are diverse sorts of blockchain structures, i.e., open, isolated, and consent. Open blockchains permitted anybody to connect. There are more often than not permissionless which each client has risen to right. Isolated blockchains could be private blockchains in which security is vital. Hence, each taking part hub is pre-selected and checked. They are accessible and the client doesn't get fixed rights within the database [33].

Among the critical highlights of blockchains, distributed by allowing the record available by each member, permanence, so blockchains are about outlandish to alter and are censorships-resistance, accessibility by giving all block a memory space of the blockchain to urge get to all times-stamped exchange record, and namelessness, which all clients can connect with the blockchain with a created address, that does not uncover the genuine character of the client [33]. Present blockchains frameworks are characterized into four parts: hybrid blockchain, open, privates, and consortium as appeared within the taking after the table. CPS is a built framework in which the physical framework is increased with cyber parts, such as processing equipment and communications arrange. These parts are exceptionally firmly coordinated with each other, which suggests the usefulness of one part is subordinate to the other components [34]. Blockchain incorporates a great potential to make unused establishments for most disseminated frameworks by productively building up belief among hubs. It may be an essential innovation to empower decentralization and play an imperative part in CPS space because of its characterizations as illustrated in Table 1.

Blockchain is the developing disturbing innovation having the potential to construct the dispersed belief by guaranteeing the unchanging nature of the data and exchange among the taking an interest organize. The provenance of the exchange gets to be conceivable, and one can follow the source and validity of the data and related substances within the organization [34, 35]. The integration of blockchain innovation with the cyber-physical society will empower the cyber-physical substances to take part in creating unused trade utilize cases, trade models, and shared economies.

Table 1 The characteristics of blockchain types

Types	Characteristics
Public blockchains	Give a completely decentralized arrangement, where each part can get to the blockchain substance and may take a portion within the agreement handle
Private blockchains	Committed to single venture arrangements and utilized to keep track of information trades happening between diverse divisions or people. Each member requires assent to connect the organization and be viewed as a part when it is being followed
Consortiums blockchain	Permission to organize and open as it were to a favored bunch. It is utilized as an examinable and dependably harmonized conveyed database that keeps track of client's information trades
Hybrid-blockchain	Merge the benefits of the open and private blockchain. Subsequently, open blockchains are utilized to form the record completely open, with private blockchains working within the context that can rule the alterations within the record

Blockchain kills the dangers related to centralized engineering. This up-and-coming innovation gives web users the capability to make esteem and verify advanced data. It can transform differing commerce applications set, extending from allocated budget to information administration and markets forecast [36]. Conveying blockchain in IoT frameworks has a few points of interest, counting, security based on the cryptographical plan, permanent information structure, exchanges and/or information confirmed by the framework, an add up to requesting of exchanges or pieces, disseminated nature (no single point of disappointment), P2P interaction, and fault-tolerance due to the utilization of conveyed agreement and gossip-based communication convention.

7 Blockchain for IoT-Based CPS Framework

Blockchain Innovation and Web of Things (WoT) are encountering exponential development in later a long time. Blockchains have been seen as standard innovation that has society revolution potentiality. IoT enables any protest to be able to put through and communicate through the Web, in this manner, bridging the physical and advanced universes, whereby information can be assembled and dispersed into gigantic data framework at the high level of granularity [37]. IoT cannot ensure security by plan, making its applications powerless particularly to security dangers. By the Blockchain Terminals (BCTs) abilities, it's able to achieve utilized as the fundamental portion that could fathom numerous inadequacies services of IoT. Hence, the current industry can be made strides, and models for modern commerce could be carried into reality. Despite third parties would be needed to ensure belief of trade exchanges may be noteworthy esteem towards commerce development in numerous zones [38].

Blockchains could be utilized to observe and monitor the measurements of sensors' data and avoid replication of any malicious IoT devices deployed to inject malicious data. This could be difficult, and a decentralized administration could be well distributed to support IoT devices' identities, authentications, and transparent privacy data exchange. A conveyed belief innovation, guaranteeing adaptability, security, and protection, may be established for the development of IoT applications, BCT gives a secure capacity for delicate information and makes it available among IoT clients. Thus, by plan, it can guarantee security, and nonappearance of single focuses of disappointment [39]. BCT can serve two principal parts to supply trusted information from its secured blocks and trusted of located processing, which ensures processes and functions to be processed reliably over members. Cyber-Physical Frameworks (CPS) may be a major innovation that contributes massively to IoT headway in fabricating frameworks. IoT device's nature has its special features that impact on the BCTs applications as takes after [40].

- A. **Dispersion:** A bounty of clients is conveyed in topographically dispersed areas. Computations and benefit arrangements may arrange at the exceptionally systems edge or at center stages, i.e., clouds. Wealthy intuition and interoperation are expected and require the exchange of a huge data amount.
- B. **Processing Capabilities:** IoT clients extend from little implanted utilities with limited resources to effective cloud servers, i.e., fog computing. IoT frameworks as a rule comprise servers, clients, and their structure by using an administration computer program to supply IoT administrations to exterior devices and edges.
- C. **Data and Information:** The rate of information delivered by keen clients is very fast growing because of the predominant organizations and extension of services for IoT.
- D. **Heterogeneities:** IoT frameworks comprise numerous sorts of clients with distinctive equipment and computer programs and take after diverse standards/protocols. A few parts of systems may be confined in an unexpected way beneath nearby laws and controls.
- E. **Dynamicity:** IoT situations are exceptionally energetic. Clients are risen, ended, associated, or disengaged from an arrangement at any time. Clients, computer programs, and systems may end up flawed or attacked. The instability of clients is exceptionally normal in IoT networks.
- F. **Motilities:** A few clients such as smartphones and others associated by nature with the vehicle have a great portability degree, inferring that it could be beneath distinctive spaces of organizations throughout entire lifecycles.
- G. **Administrations Ubiquity:** IoT provides an exceptional gigantic degree of benefits arrangements which could be open over the universe. Numerous IoT provides comparable features with distinctive necessities and quality of services (QoS).

8 Blockchain IoT-Based CPS Applications

CPS and IoT empower inventive applications, the essential components of a CPS or IoT run from physical components, and their related sensors and actuators, through control frameworks and analytics, to the by and large optimization and client usefulness, with confirmation that prerequisites have been fulfilled [41]. The CPS System portrays the work and work items of investigation, organized by groupings of exercises or features of modes of considering like conceptualization, realization, and confirmation, in addition to perspectives including collections of concerns like utilitarian, commerce, human, dependability, timing, information, composition, boundaries, and lifecycle that bolster framework building investigation, plan, advancement, operation, and approval and affirmation of CPS/IoT [42].

CPS envelops opened and closed loops control frameworks, whereas IoT ordinarily centers on opened loop frameworks, and covers with CPS, since IoT enables to watching the objects in the physical world. In addition, to make communication capabilities, and capturing the required information for overseeing the things that cannot be productively overseen nowadays [43]. Indeed, even though IoT initially focused on distinguishing proof and observing advances. Nowadays IoT enables the control of the physical frameworks by the integration with the RFID frameworks and sensor systems to be specific RFID sensor networks. The half-breed physical and consistent character of CPS/IoT frameworks gives a binding together that implies for categorizing the different components of CPS/IoT frameworks. Physical components related to components within the physical domain are habitually given the bland name things as in IoT, in addition to the term physical in cyber-physical frameworks [44].

The consistent parts of the IoT/CPS framework are understood within the terms Internet and cyber individually, which includes program layers to provide frameworks working, and applications. Moreover, it enables to provide equipment parts from control supplies, communications to peripherals as well, in addition, to organize and communications texture, comprising the frameworks, services, etc. Accordingly, different applications are related to IoT/CPS framework such as health care, industrial control, transportation, and vehicles networks, in addition to the smart grid [45]. All of these applications are related to the parts of CPS/IoT frameworks used to connect all physical and coherent domains such as sensors, actuators, and transducers. In CPS/IoT framework, transducing parts are sensors that enable to accumulation of data around the physical state of the framework for utilization in consistent forms. The actuators, act in reaction to consistent framework yields and apply vitality to modify the physical state of the framework. The development of combined physical and coherent intuition of people with their environment IoT and CPS frameworks contain all mentioned parts, which are requiring to be in secure mode operations in a frame covered by blockchain [46].

8.1 Blockchain in Healthcare Applications

Health care is a potential application considering the blockchain. The individual well-being records of medical and healthcare operations data should be managed securely. The individual records encoding enables to put away utilizing blockchain, in addition to providing a private key which would permit as it were particular people to get records. Essentially, the same convention can be connected to conduct an investigation where individual records are utilized through Health Insurance Portability and Accountability Act (HIPAA) laws to guarantee the secrecy of the information [47]. The records of patients can be sent within the blockchain concept to security suppliers or a specialist to send health records to the respective parts securely. To shift to a blockchain concept in health care, it is necessary to link heterogeneous frameworks with the health information management and well-being center and increased scrutiny of electronic welfare records (EHRs). Electronic medical records (EMR) can also be exchanged [47, 48].

In health care, an electronic medical record (EMR) provides information about patients' medical and treatment history simultaneously. Electronic health records focus on the complete well-being of previous standard clinical patient information collected within the provider's office and encompass a broader view of patient care [49]. Keeping the importance of medical information secure is the foremost well-known blockchain healthcare application. Security is an important issue within the healthcare industry. In the period between a year from 2009 to 2017, more than 176 million persistent records were uncovered in information breaches. The culprits stole credit cards and managed account data, as well as well-being and genomic testing records.

In health care-based CPS, efficient discussion making can be achieved by supporting data acquisition for the integration of different healthcare data resources such as digital patient records, biosensors, or smart healthcare environment devices. By implementing IoT-related CPS in the holistic healthcare field, autonomous medical devices can be managed interoperable and adaptively with computing and control systems and implantable devices [50]. The healthcare CPS infrastructure consists of components related to controlling and applications, medical sensors, as well as data storage and cloud computing as shown in Fig. 5. It is necessary to pay attention to the mechanisms of securing and encryption of CPS systems due to the privacy and sensitivity of medical information, especially as it is related to cloud systems and IoT applications. Also, scalability and high accessibility need to put limits on resources, especially for hardware.

In the medical field, the confidentiality of medical information is one of the important criteria as it constitutes a burden on health care systems, so data privacy at the application and infrastructure level for CPS systems is one of the most important requirements. Blockchain's capability to keep an upright, decentralized, and straightforward log of all persistent information makes it an innovation overflowing for security applications. Although the blockchain is straightforward, it is characterized by privacy and the ability to hide complex and secure information and

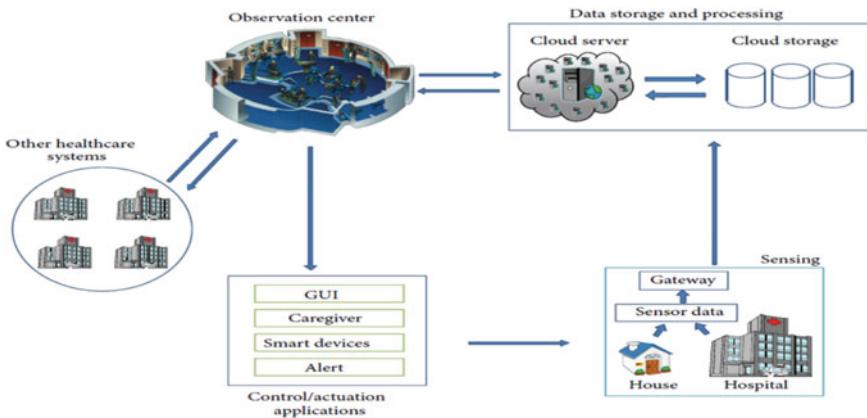


Fig. 5 CPS architecture for healthcare application

provide insurance services for therapeutic information. The decentralized nature of the blockchain allows for the same data to be shared quickly and securely between the different parts of the health system, including patients, specialists, and healthcare providers [50]. Miscommunication between therapeutic experts costs the healthcare industry a stunning \$11 billion a year. The time-consuming handle of getting to a patient's therapeutic records debilitates staff assets and delays understanding care. Blockchain-based therapeutic records offer a remedy for ills. The decentralized nature of innovation provides a single environment of continuous information that can be quickly and effectively consulted by professionals, clinics, and pharmaceutical professionals, demonstrating the potential of blockchain to serve fast and secure analytics processes [51].

8.2 *Blockchain Applications in Industrial Control Systems (ICS)*

ICS could be a common term that includes a few sorts of frameworks such as control, counting information administration, conveyed control, and others such as Programmable Logic Controllers (PLC) within the mechanical segments and basic frameworks. An ICS comprises combinations of control components that act together to realize a mechanical objective execution. ICS control mechanical forms are regularly utilized in electrical, water, oil characteristic gas, chemical, transportation, pharmaceutical, in addition to fabricating businesses [52]. ICS is the basic operation of industrial frameworks that are frequently profoundly interconnected and commonly subordinate. Since there are numerous distinctive sorts of ICS with shifting levels of potential chance and affect, researchers ought to pay consideration to ICS organize security.

In ICS, sensors and actuators are controlled by the PLC or Distributed Control System (DCS) and may also be connected to the control of system networks and IoT, in addition to Human Machine Interface (HMI). The operations of such interfaces are required to be protected in the levels of operational processes and information exchanged between corporate and control system networks. Accordingly, interfaces with the real world may have serious problems of vulnerabilities and their exploitation by attackers [51, 52]. Some statistics are showing that the rate of attacks on ICS devices in 2020 amounted to 33.4%. During the years from 2016 to 2020, the percentage of attack rate is increased dramatically as shown in Fig. 6. According to these statistics, and for security sure, blockchain innovation offers effective solutions to lock down ICS systems within a framework that creates a movable information record that is reproduced and shared between individuals in organizational and operating agreement accounts that can ensure security of tool exchange information in such systems. Blockchains enable to organization security of ICS which includes a huge sum of information preparation, real-time prerequisites of the higher frameworks, and have to be set up a shorter interim overhaul innovation framework [53].

In Industrial Control System (ICS), the programmed control framework comprising of computer gear and mechanical handle control components. The mechanical control preparation incorporates real-time information collection,

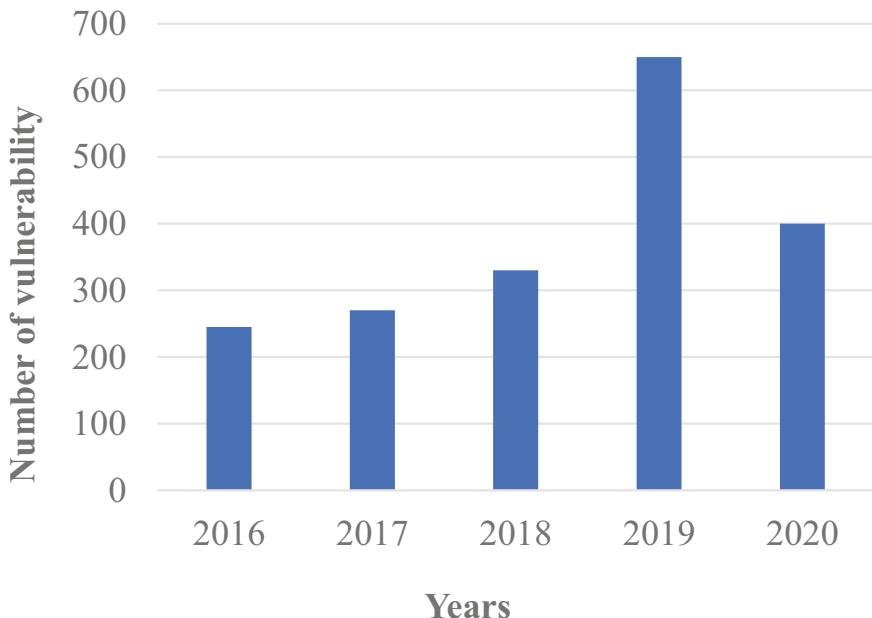


Fig. 6 Number of reported ICS vulnerabilities between 2016 and 2020

observing, arrangement to attain the robotics observing. Mechanical control framework habitually happens to arrange security episodes, which has stirred the consideration of different nations, specialists, analysts, and engineers who are committed to fathoming mechanical control framework arrange security issues [54]. The scattered capacity and decentralization of the piece chain development meet the security necessities of the mechanical control system organization. The blockchains innovation combined with disseminated capacity innovation is utilized to build a P2P organize in ICS, by which the mechanical gadget exchange information can be put away in Blockchains securely. Through the complex confirmation instrument, the blockchains can keep up the keenness and consistency and can accomplish effective and solid transmission and trade information [54].

Blockchain enables to make mechanical gadget exchange and information trade handle straightforward and spare fetched. Moreover, it can computerize execute cleverly contract by putting away, confirming, and analyzing the mechanical gadget exchange information without losing information privacy. The use of blockchain innovation with ICS proficiency can set up a credit component in a conveyed industrial IoT, to utilize of piece chain records to screen and oversee brilliantly clients, brilliantly contracts can control the behavior of shrewdly clients, which can illuminate mechanical control framework organize security issues [55]. Blockchain can provide a dispersed information capacity to preserve a dependable database, which can adjust to the mechanical control framework organize data security. In addition, with cryptography innovation blockchain can guarantee that information industrial control systems have a complete handle of secure [56].

Blockchain/ICS framework enables connection of gadget hubs and each client's hub executes savvy contracts and records the exchanges information. The Blockchain is reproduced among the gadget hubs within the ICS network. Any gadget hub within the ICS arrange can record all exchanges information [57]. As a result, the gadget hubs on the ICS arrange to add approved, commonly concurred upon exchanges. The reason for an agreement component calculation is to permit the secure overhauling of a state. Agreeing to state move rules, where the proper to perform the state moves is dispersed among the ICS data set. The ICS information set can be clients which are given the correct to collectively perform moves through a calculation [58].

Blockchain innovation has other potential applications for ICS, such as the assurance and confirmation of gadget firmware and application program overhauls [59]. As ICS clients have secured their systems, aggressors have taken to other strategies to penetrate frameworks. A blockchain organized basically may be a set of non-trusting hubs connected with the other no trusted hub with a shared database, each gadget hub contains whole database exchange data which is called one piece and one record, all gadget hub in ICS shaped blockchains and conveyed record [60]. In an arrangement to anticipate the aggressor from ejecting in this dispersed environment, and in an arrangement to assist the arrangement reach agreement, each blockchain organized must set up certain rules that each gadget hub exchange ought to take after [61]. These rules are modified into each blockchain client hub, which at that point employs them to choose whether an approaching exchange is substantial, and thus whether it ought to be transferred to the organization or not.

8.3 *Blockchain for Transportation Applications*

The CPS system and its applications in intelligent transportation (ITS) are among the most important issues related to the concept of cyber in transportation systems. The combination of vehicle and organized communication innovations have pushed the boundary of the following era, associated vehicles [62]. This applies weight to car producers to offer imaginative items and administrations in that space. Whereas the associated vehicle and roadside foundation are physical substances, the Vehicular Communication System (VCS) may be an arranged stage that gives Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications. With the assistance of the improvement of dispersed computing foundations for CPS, the vehicle gets to be a stage able of getting data from its peers and the environment producing its claim information, such as driver behavior and car state and transmitting information to other vehicles, roadside foundation, or third parties in arrangement to move forward street security, contamination control, protections data, and activity effectiveness [63].

In development, the IoT advancement is driving customary VCS to ask around and headway towards the internet-of-Vehicles (IoV). The IoV applications depend on the trade of Fundamental Security Messages (BSMs) which contain vehicle status data such as area, speed, and vehicle measurement. Because of the reality that numerous applications and administrations make utilize of BSM which contains vehicle personality, area, and other individual information VCS faces the chance of not as it was unveiling delicate data approximately vehicles and clients, but too of antagonistic control of character and area data [64]. In a conventional VCS structure, a central supervisor such as a Certificate authority (CA) or Public-Key infrastructure (PKI) is outlined to oversee nom de plumes certificate centrally. Be that as it may, a centralized arrangement can be exceedingly unsteady, have more adaptability, and speaks to a critical single point of assault [64, 65]. Many nom de plume administration plans state that a conveyed and decentralized framework seems to accomplish superior secrecy and strength.

Unused blockchain-enabled stages will permit simple coordination of archives on a shared conveyed record, making physically printed material generally superfluous, by utilizing contracts, endorsements, and traditions clearance can be speedier and more effective, decreasing handling times for merchandise at traditions checkpoints. Organizations require overhauled, secure, and bona fide information to form choices. Blockchain guarantees reliable information over the transportation and coordination biological system since the whole organize contributes to information approval [66]. With a rising request for same-day and one-hour conveyance administrations, conventional following innovations will not scale. Blockchain innovation gives an adaptable, prompt arrangement for arranging following and confirmation.

8.4 Blockchain in Smart Grid

In later a long time, the shrewd network concept which includes communication innovation, interconnected control framework, progressed control innovation, and savvy metering has been connected to move forward the utilization of renewable vitality sources and diminish the vitality emergency by one means or another [67]. The concept of the savvy lattice has been presented as an unused vision of routine control network which offers two-way vitality and data trade in arrangement to figure out an effective way of conveying, overseeing, and joining green and renewable vitality advances, the decentralized savvy network framework with an expansive number of components and complex associations may too be security, protection, and believe bad dream which needs unused and imaginative advances [68]. Moreover, as developing and promising innovation, blockchain offers unused openings to create decentralized frameworks.

Decentralization of blockchain innovation allows for the possibility of supervision and control, where there is no need for a reliable central specialist [69]. This decentralized framework makes any framework repetitive and versatile to framework disappointment and cyber-attacks and fathoms numerous issues of the centralized framework. Even though the blockchain is at first presented and populated as advanced monetary standards, due to having its fabulous properties, it is pulling in gigantic consideration in numerous other non-monetary applications. Simultaneously, past computerized monetary standards, blockchain is additionally advancing the realization of secure, privacy-preserving, and trusted smart network advancements toward decentralization [70]. Blockchains applications within the shrewd lattice can be isolated through the diverse parts of the shrewd framework as taken after.

- A. **Power Era:** Blockchain innovation gives the dispatching offices full information around the by and large operation status of a control network in a real-time point of view. This empowers them to create dispatching plans that would maximize profits.
- B. **Power Transfer and Dispersion:** Blockchain frameworks enable computing and control centers to have decentralized frameworks that overcome most of the challenges that appear in traditional centralized systems
- C. **Power Utilizations:** Similar to the era and aspects of transportation, blockchain may be useful in this aspect by overseeing the exchange of vitality between consumers and diverse biocapacity frameworks as well as electric vehicles.

9 Challenges of Blockchain IoT-Based CPS Integration

Applications of CPSs required to be modeled according to their effect on the community and essential systems-level necessities [71]. The blockchain in IoT-based CPS management and process are related to different performance requirements such as

scalability, security, and privacy. The following sections describe the performance requirements and shortcomings of blockchain implementations.

9.1 *Performance Requirements*

The integration of blockchain with the IoT in a framework architecture is an important issue, especially in considering the CPS systems applications. The ability of Blockchain to design web situations using computers allows interaction with IoT sites remote from the system [72]. Blockchain exchanges are carefully marked, and so clients able of working with the money must be prepared with this usefulness. Is challenging to consolidate the blockchains in IoT.

9.1.1 **Scalability, Capacities, and Storages**

As expressed, the capacity and adaptability of blockchains are still beneath wrangle about, but within the setting of IoT application, the inalienable capacity and adaptability restrictions make this challenge much more prominent [73]. In this context, blockchains may show up to be unacceptable for IoT services, in any case, there are methods in which these confinements might be eased or maintained a strategic distance from through and through. Within the IoT, where clients can produce gigabytes (GB) of information in genuine time, this impediment speaks to an awesome obstruction to its incorporation with blockchains [74]. There are some uses of the blockchain that can count several exchanges at any given moment which is likely to cause problems for IoT applications. Moreover, blockchain cannot be able to store a huge amount of information like IoT. Integration of these innovations ought to bargain with these challenges.

Right now, a part of IoT information is put away and as it were a restricted portion is valuable for extricating information and creating activities [75]. The IoT includes implanted clients, communication, and target administrations (blockchain, cloud), hence reserve funds within the sum of information that the IoT gives can advantage numerous layers [75, 76]. Information compression can help transmission, preparing errands, and capacity of the tall volume of IoT data generated. Ordinary behaviors don't as a rule require additional, vital data, not at all like bizarre information. Blockchain, and particularly its agreement convention which causes a bottleneck, might moreover be adjusted to extend the bandwidth and reduce the inactivity of its exchanges thereby empowering distance with a better move to the IoT illustrated by the case of Bitcoin-N.

9.1.2 Security Capabilities

For IoT and blockchain applications, there is a need to compromise security issues at distinct levels with additional restrictions, according to the needs of clients. In addition to the need of the customer, the limitations include both the state of the resource properties of the Internet of Things, which can affect the security of data and communication [77]. The increasing number of attacks on IoT networks and their real effects makes it necessary to configure IoT with more modern security. Many professionals see blockchain as a key innovation to provide the security changes needed in the IoT. In any case, one of the biggest challenges in integrating the IoT with the blockchain is the consistent quality of the data that the IoT produces. Blockchain can guarantee that information within the chain is unchanging and can distinguish their changes, all things considered when information arrives as of now undermined within the blockchain they remain degenerate. Degenerate IoT information can emerge from numerous circumstances separated from pernicious ones [78].

The prosperity of the IoT design is influenced by numerous components such as the environment, members, vandalism, and the disappointment of the clients. Sometimes the clients themselves and their sensor and actuator come up short to work legitimately from the beginning. This circumstance cannot be determined until the tool in the address has been tried, or sometimes it works properly for some time and changes its behavior for various reasons related to short circuit, disengagement, and old quality modification. In expansion to these circumstances, numerous dangers can influence the IoT such as listening in, controlling, or refusal of benefit [79]. Accordingly, IoT clients must have been thoroughly experimented with at some point recently on their integration with the blockchain. Plus, they must be found and categorized in the right place to avoid harm. These clients are more likely to get hacked because their necessities restrict firmware upgrades, preventing them from activating due to conceivable bugs or security breaches. Besides, it is in some cases troublesome to overhaul clients one by one, as in worldwide IoT arrangements. To do this, the components of runtime refresh and reconfiguration must be set within IoT to keep them running for additional minutes [80]. IoT and blockchain integration could also have implications for IoT communications.

Right now, IoT application conventions such as Messages Queues Telemetry Transports (MQTTs) and Constrain Applications Protocol (CoAP) make utilize of other security conventions such as Transport-Layer Security (TLS1.2) or Datagram-TLSs (DTLSS) to provide communications security. Secure agreements are complex and glamorous in terms of scaling to require centralized management and governance of the main organization, usually with a PKI. Within the blockchain organized each IoT gadget would have possessed World Especial Identifiers (GUIDs) and topsy-turvy key match introduced once associated to the organizing. This would streamline current security conventions which more often than not have to trade public-key infrastructures (PKIs) certificates and would permit them to be utilized in clients with lower abilities [81].

9.1.3 Data Confidentiality and Obscurity

Numerous IoT applications work with private information, for the occasion when the gadget is connected to an individual, such as within the eHealth situation. Blockchain is displayed as a perfect arrangement to classify the IoT character administration, be that as it may as in Bitcoin, there may be an application where secrecy should be ensured [82]. Such applications as in the case of wearable IoT devices that able to hide the individual's identity when sending individual information.

9.1.4 Intelligent Contract

Smart contracts are distinguished as the implementation applications of blockchain innovation that can be utilized in IoT applications. However, working with smart contracts requires the use of extraordinary resources that can give real information to the world in a reliable manner [83]. Due to the instability of the IoT, the approval of these smart contracts can be compromised. In addition, getting to different information sources may over-burden these contracts. These days, intelligent contracts are dispersed and distributed, but they don't share assets to disseminate errands and address a huge amount of calculations. On other hand, savvy contract execution is wiped out fair a single hub though at the same time the manipulation of the code is done by different hubs. This dispersion is as it was done for the approval preparation, rather than utilizing it to disseminate assignments [84].

The IoT has utilized the dispersed cloud computing capabilities and huge information to extend its preparing control. Since then, information mining procedures have been able to process IoT information as a whole, empowering distant and improved the IoT understanding, i.e., the handling control extended by cloud computing [85]. Huge information has empowered the preparing of huge sums of information at the same time, permitting information to be extricated from expansive information sets, which was already exceptionally difficult to realize. Within the blockchain and IoT integration, the keen contract ought to use the nature have distributed to empower the handling abilities given in other standards (fog computing and huge information) and required within the IoT and are categorized as explained in the next section, i.e., identities-based attack, manipulations-based attack, cryptanalytic attack, reputations-based attack, and services-based attack [86].

- A. **Identities-Based Attacks:** forge identities to pretense as authorized clients, to have access to processing and system. Such attacks like Main attacks, Re-play attacks, Impression attacks, and Sybil attacks [87].
- B. **Keys Attacks:** attacks occurred in the system context associating electric vehicle and piles' charge, as follows: the secret keys of electric vehicles that have been utilized for a long time leak, the attackers could imitate these electric vehicles to cheat other vehicles. A reciprocated privacy mechanism between the electric vehicle and piles charge is required [88].

- C. **Re-play Attacks:** These attacks parody two devices' identities, interrupt the traffic, and re-play their data to destination with no modifications. Encryption of elliptical diagram could be utilized to compute hash function [86].
- D. **Impression Attacks:** Kind of attacker's attempt to deception as a genuine client to execute illegal processes. Encryption of elliptical diagram has been utilized to compute the hash function to avoid such attacks [87]. In addition, the method of preserving the privacy of the users' data with the cluster is used to guarantee impression attack preservation.
- E. **Sybil's Attacks:** attackers create several false IDs. By executing several network transactions and traffic, the attackers could obtain a huge effect on the system [89]. Sybil's attacks guarantee that agent who utilizes resource from the cyber community also contributes back.
- F. **Data False-Injections Attacks:** The goal of these attacks is to adverse the integrity of system control data to disturb the decisions of the control system [86].
- G. **Tamper Attacks:** The attackers may tamp the transaction of bitcoin, the addresses of bitcoin, amount, and/or any data after log in. To avoid these types of attackers, a cryptosystem of public keys is utilized where it should be harmonious with the present systems of bitcoin [88].

9.2 *Shortcomings of Blockchain Implementations*

The most drawback of the Blockchain is the tall vitality utilization. The utilization of control is required for tracking a real-time record. Each time the modern node is made and within the same time, it connects with each and another hub. In this way, straightforwardness is made. The network's mineworkers are endeavoring to unravel a parcel of arrangements per second in endeavors to approve exchanges [90]. They are utilizing considerable sums of computer control. Each hub is giving extraordinary levels of blame resilience, guarantees zero downtime, and is making information put away on the blockchains until the end of time unalterable and censorship-resistance. But these activities burning power and time is inefficient when each hub rehashes the accomplishment of the Agreement. The signature confirmation is the blockchain challenge since each exchange must be marked with cryptographic conspire, the huge computing control is vital for the calculation prepared for the sign. It is one of the motives for tall vitality utilization [91].

Another issue of the blockchains is part of the chain opportunity. The hubs, which are working to the ancient program, won't acknowledge the exchanges within the modern chain. This chain is made with a similar past as the chain which is based on the ancient computer program. It is named the fork. There are two fork's sorts the delicate fork and the difficult fork. The delicate fork sets up the modern run the show set to the squares within the convention. The hubs are upgraded to uphold the delicate fork's rules. In case the square, which was considered substantial sometime

recently, does abuse the modern delicate fork rules, the square won't consider after the delicate fork actuation.

For illustration, the delicate fork is confining the piece estimate until 500 kB, but some time recently was the 1 MB. It implies that the squares, which are bigger than 500 kB, won't be substantial within the modern chain after overhauls. The difficult fork has loosened the run the show set to the squares within the convention [92]. This preparation is the same as the delicate fork preparation, but the esteem and result of it are the inverses. The difficult fork is expanding the square measure to 1 MB from 2 MB. If the piece is gone through all the rules of the difficult fork, the piece will be accepted, indeed on the off chance that the square was not within the chain before. Another issue of the blockchains is the adjustment between the nodes' amount and the favorable costs for clients. Presently there are the hubs that are needed for the blockchains to accurately and effectively work. In this case, the costs are higher, since the hubs received higher rewards; but the exchanges are completed more gradually since the hubs don't work seriously [93].

The blockchains have developed when the unused squares partner to the chain and the computing prerequisites increment. Not all hubs can give with the essential capacity. There are two issues, the primary is the littler record since the nodes cannot carry the total duplicate of the blockchain and it breaks the permanence and straightforward of the blockchains. And the moment is the blockchains get to be a more centralized framework. The tall costs are an enormous impediment to the Blockchain [94].

9.3 Security Issues

The blockchains can be adverse by the various vulnerable, which are connected with the proof-of-Works (PoWs) and proof-of-stakes (PoSs) procedures. Most of these vulnerabilities are near to be impractical. Adverse of 50% would occur when two miners are computing the block hash in the meantime and have similar outcomes. In these cases, the blockchain would divide and as the consequence, each client has two different chains, and both are counted correctly [95]. Double-spending is principles of these attacks is similar to the former attacks, but one can use the chain split to spend the money again. Sybil's attacks are conceivable when the device accepted many incidents since the network wouldn't genuinely differentiate the physical devices.

Sybil's attacks could assist to fill the blockchains with clients below its control [96]. It also could employ the previous two attacks and the capacity to observe all transactions with extraordinary programs. DDoS attacks comprise an expansive sum of comparative demands. There's the security within the DDos's assault estimate of the piece up to 1 MB, a measure of each script up to 10 Kb, up to 20 Kb of the marks can check and maximize the numerous signatures is 20 keys. cryptographic Splitting is conceivable if utilizes quantum calculations that can break the RSA encryptions [96, 97]. The researchers work on the cryptographic calculations, which are based on the hash capacities.

9.4 Limitation of Public-Key Infrastructure

Whereas PKIs nowadays holds the security angles of these packets, it endures from the same impediments as any centralized confirmation framework. Moreover, a centralized PKIs needs genuine data almost in ground reality because it doesn't have the detecting abilities accessible on the vehicle. Blockchains handle a cutting-edge motivation for the vehicles. Within the case of communicated vehicles, the exchanges shared between vehicles are the essential security message, which comprises data around the estimate, location, speed, and vehicle heading. These messages are digitally marked and the signature is approved by the PKIs [98]. They got to be kept up in a time-sequenced chronicled way within the envelopes for use-cases related to law requirement and protections claims. These exchanges are approved in real-time for prompt use-cases related to higher levels of computerized driving. Furthermore, these exchanges ought to not be altered at any time within the future, as they may be required for legal and protection claim reasons [99]. All of these prerequisites, make blockchains a reasonable alternative to consider for exchange administration in associated vehicles.

10 Effective Adoption Barriers of Blockchain IoT-Based CPS Technology

Despite the value of blockchain-based IoT-based CPS innovation; the selection rate is or maybe moderate and may be ruined by covered-up components that obstruct firms' choices. The method of introducing a recent innovation into an industry can be complex and lengthy, as suggested by the scourge hypothesis. Some companies may want to order the basic step as an early adopter, while others may prefer to play it safe [100]. Others may consider their options, either because they have restricted assets, or because the benefits collected are not convincing enough.

Security and defenselessness were found to be barriers to choose from within the innovative setup, and the must trade-offs between security and execution. Conniving is still conceivable through an agreement among members of 51% assault [100]. Blockchain allows providing a high level of security and awareness by not tying choice trends. The need to unify the degrees of safety may be fulfilled when another point of resistance appears. However, in the general case, there will be no uniform degrees of computational unification [101]. Blockchain cannot function well due to the complexity of the programming framework due to the possibility of errors in calculations and delays by programmers [102].

Other components to consider are adaptability square estimate and speed. These requirements can be expressed as the ability to conduct the exchange and complete its objectives in an appropriate period. Right now, a blockchain enables to provide seven exchanges per moment on normal, and the square measure is constrained to just one megabyte. In the case of more widespread use of blockchain, this issue should

be taken care of with caution. Blockchain within the supply chain requires embed regulation [103]. Strong support must also be provided through the collaborating companies to put this innovation into practice.

The negative differences related to the blockchain due to Bitcoin remain strong. The terms blockchain and Bitcoin are still understood to the contrary. It may take time to spread the idea that blockchain and Bitcoin are not the same. Blockchain has appeared in the Internet of Things recently, and it still faces problems, drawbacks, and several limitations related to the selection of targeted frameworks in various applications [104].

Additionally, another requirement to consider when achieving a blockchain innovation is interoperability or compatibility. Companies must either have blockchain-based arrangements or build them to align with their frameworks. In expansion, the coordination blockchain requires adjustments to be made to a bequest framework [105, 106]. With the use of blockchain in companies and institutions, usage costs may change due to some basic components, counting equipment, computer software, recording, and internal preparation, and include both opportunity costs and bookkeeping costs [107]. Blockchain is accepted to be an innovation with tall up-front speculation costs, even though it brings almost focal points in fetched diminishment [108].

11 Conclusions

Maintaining them may be a critical innovative insurgency. Blockchain is here to remain. In general, changing blockchain innovation without ensuring it is adequately operational or applying it to scenarios where losses do not compensate for progress is considered high risk. Therefore, the benefits of applying blockchain to the IoT should be carefully analyzed and taken with care. The combination of blockchain, CPS, and IoT can be very capable, as blockchain can give flexibility to assaults and the capacity to associate with peers in a solid and auditable way. Blockchain's proceeded integration into the IoT space will cause noteworthy changes over different businesses bringing modern commerce models and making us reexamine how existing frameworks and forms are actualized. In this chapter, we have begun by recognizing cyber-physical framework transformation and the multi-paradigm demonstrating cyber-physical frameworks.

At that point plan of CPS based on the Framework of Frameworks moreover, the building layers one by one concerning their duties. Receiving blockchain for CPS isn't clear either and has it possessed challenges. More adaptability, tall idleness, more throughput, computationally costly agreement instruments, belief and protection related issues of blockchains are critical boundaries to blockchain selection for CPS we have afterward begun our chapter on CPS applications that have one-of-a-kind imperatives and prerequisites. As blockchain is a rising innovation with the potential to make strides in the execution of CPS, numerous inquire about questions and opportunities exist within the ranges of planning novel blockchain instruments

for CPS and embracing blockchains for CPS applications. It is still within the early stages of creating piece chains, and these impediments will inevitably be overcome, opening the way as well numerous conceivable outcomes.

References

1. Rathore H, Mohamed A, Guizani M (2020) A survey of Blockchain-enabled cyber-physical systems. *Sensors (Basel)* 20(1):282. Published 2020 Jan 3. <https://doi.org/10.3390/s20010282>
2. Boubacar ElMamay S et al (2020) A survey on the usage of Blockchain technology for cyber-threats in the context of industry 4.0. *Sustainability* 12:9179
3. UI Hassan M, Rehmani MH, Chen J (2019) Privacy preservation in blockchain-based IoT systems: integration issues, prospects, challenges, and future research directions. *Future Gener Comput Syst* 97:512–529
4. Bouachir O, Aloqaily M, Tseng L, Boukerche A (2020) Blockchain and fog computing for cyber-physical systems: the case of smart industry. [arXiv:2005.12834v3,12](https://arxiv.org/abs/2005.12834v3)
5. Farouq M, Osman N, A. Elamin AA, Sayed Ali Ahmed E, Saeed RA (2021) Cyber-physical system for smart grid. In: Luhach A, Elçi A (Ed.), Artificial intelligence paradigms for smart cyber-physical systems (pp 301–323). IGI Global. <https://doi.org/10.4018/978-1-7998-5101-1.ch014>
6. Mahboub SA et al (2021) Smart IDS and IPS for cyber-physical systems. In: Luhach AK, Elçi A (eds) Artificial intelligence paradigms for smart cyber-physical systems, IGI Global, 2021, pp 109–136. <https://doi.org/10.4018/978-1-7998-5101-1.ch00>
7. Nurelmadina N, Hasan MK, Mamon I, Saeed RA, Akram K, Ariffin Z, Sayed Ali E, Mokhtar RA, Islam S, Hossain E, Arif Hassan Md (2021) A systematic review on cognitive radio in low power wide area network for industrial IoT applications. *MDPI Sustain*
8. Yaacoub JA, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M (2020) Cyber-physical systems security: limitations, issues and future trends. *Microprocessor Microsyst.* 2020
9. Salih Ahmed R, Sayed Ali Ahmed E, Saeed RA (2021). Machine learning in cyber-physical systems in industry 4.0. In: Luhach AK, Elçi A (Ed), artificial intelligence paradigms for smart cyber-physical systems (pp 20–41). IGI Global
10. Liu Y, Peng Y, Wang B, Yao S, Liu Z (2017) Review on cyber-physical systems. *IEEE/CAA J Automatica Sinica* 4(1)
11. Carreira P, Amaral V, Vangheluwe H (2020) Multi-paradigm modelling for cyber-physical systems: foundations. In: Carreira P, Amaral V, Vangheluwe H (eds) Foundations of multi-paradigm modelling for cyber-physical systems. Springer
12. Amrani M et al (2019) O wards a formal specification of multi-paradigm modelling. In: Proceedings of models 2019. Workshop MPM4CPS, pp 418–423, Munich, Sep. 2019
13. Tekinerdogan B et al (2020) Book: multi-paradigm modelling approaches for cyber-physical systems 1st Edition. Elsevier, Academic Press Date: 24th November 2020. ISBN: 9780128191064
14. Carreira P, Amaral V, Vangheluwe H (2018) Foundations of multi-paradigm modelling for cyber-physical systems. Springer, 2018. ISBN 978-3-030-43946-0
15. Chamberlain R, Taha W, Törngren M (2018) Cyber-physical systems. Model-based design. 8th International workshop, CyPhy 2018, and 14th international workshop, WESE 2018
16. Luis M, António J, Nazanin V, Shirin N (2016) Technological innovation for cyber-physical systems. 7th IFIP WG 5.5/SOCOLNET advanced doctoral conference on computing, electrical, and industrial systems, DoCEIS 2016, Costa de Caparica, Portugal, April 11–13, 2016, Proceedings
17. Nazarenko AA, Ali Safdar G (2019) Survey on security and privacy issues in cyber-physical systems. *AIMS Electron Electr Eng* 3(2):111–143

18. Ahmed ZE, Saeed RA, Ghopade SN, Mukherjee A (2020) Energy optimization in LPWANs by using heuristic techniques. Book Chapter (Ch 11) In: Chaudhari BS, Zennaro M (eds) LPWAN technologies for IoT and M2M applications, ISBN: 9780128188804, Elsevier, March 2020
19. Rasheed A, San O, Kvamsdal T (2019) Digital twin: values, challenges, and enablers. [arXiv: 1910.01719v1](https://arxiv.org/abs/1910.01719v1), 3 Oct 2019
20. Amrani M, Blouin D, Heinrich R, Rensink A, Vangheluwe H, Wortmann A (2019) Towards a formal specification of multi-paradigm modelling. 2019 ACM/IEEE 22nd international conference on model driven engineering languages and systems companion (MODELS-C), Munich, Germany, 2019, pp 419–424
21. Ferrer BR et al (2018) Towards the adoption of cyber-physical systems of systems paradigm in smart manufacturing environments. 2018 IEEE 16th international conference on industrial informatics (INDIN), Porto, 2018, pp 792–799
22. Ghorpade SN, Zennaro M, Chaudhari BS, Saeed RA, Alhumyani H, Abdel-Khaled S, Enhanced differential crossover and quantum particle swarm optimization for IoT Applications. In: IEEE Access, <https://doi.org/10.1109/ACCESS.2021.3093113>
23. Hassan MB, Alsharif S, Alhumyani H, Sayed Ali E, Mokhtar RA, Saeed RA (2021) An enhanced cooperative communication scheme for physical uplink shared channel in NB-IoT. *Wirel Personal Commun* 116(2)
24. Assaad MA, Talj R, Charara A (2017) A view on systems of systems (SoS). 20th world congress of the international federation of automatic control (IFAC WC 2017)—special session, Jul2016, Toulouse, France. hal-01741416
25. Dong D, Xiong H, Castañe GG, Morrison JP (2018) Cloud Architectures and Management Approaches. In: Lynn T, Morrison J, Kenny D (eds) Heterogeneity, high-performance computing, self-organization, and the cloud. palgrave studies in digital business & enabling technologies. Palgrave Macmillan, Cham
26. Jurcut A, Niculcea T, Ranaweera P et al (2020) Security considerations for internet-of-things: a survey. *SN Comput SCI* 1:193
27. Hassan MB, Sayed Ali E, Mokhtar RA, Saeed RA, Chaudhari BS (2020) NB-IoT: concepts, applications, and deployment challenges. Book Chapter (Ch 6) In: Chaudhari BS, Zennaro M (eds) LPWAN technologies for IoT and M2M Applications, ISBN: 9780128188804, Elsevier, March 2020
28. Bordel B, Alcarria R, Robles T, Martín D (2017) Cyber-physical systems: extending pervasive sensing from control theory to the Internet-of-things. *Pervasive Mob Comput* 40:156–184
29. Rathore H, Mohamed A, Guizani M (2020) A survey of Blockchain-enabled cyber-physical systems. *Sensors* 20(1):282
30. Lim SY et al (2018) Blockchain technology the identity management and authentication service disruptor: a survey. *Int J Ad Sci Eng Info Tech* 8:4–2
31. Ben Fekih R, Lahami M (2020) Application of Blockchain technology in healthcare: a comprehensive study. In: Jmaiel M, Mokhtari M, Abdulrazak B, Aloulou H, Kallel S (eds) the impact of digital technologies on public health in developed and developing countries. ICOST 2020. Lecture Notes in Computer Science, vol 12157. Springer, Cham
32. Namasudra S, Deka GC, Johri P et al (2020) The revolution of Blockchain: state-of-the-art and research challenges. *Arch Comp Methods Eng* (2020)
33. Makridakis S, Christodoulou K (2019) Blockchain: current challenges and future prospects/applications. *Future Internet* 11:258
34. Alsolami F, Alqurashi FA, Kamrul Hasan M, Saeed RA, Abdel-Khalek S, Ishak AB (2021) Development of self-synchronized drones' network using cluster-based swarm intelligence approach. *IEEE Access* 9
35. Francisco et al (2020) Blockchain from the perspective of privacy and Anonymisation: a systematic literature review. *Sensors*
36. Wattana V, Tharwon A, Danupol H (2019) when blockchain meets internet-of-things: characteristics, challenges, and business opportunities, *journal of industrial information. Integration* 15:21–28

37. Panarello A, Tapas N, Merlini G, Longo F, Puliafito A (2018) Blockchain and IoT integration: a systematic survey. *Sensors (Basel)* 18(8):2575. Published 2018 Aug 6
38. Baldiucini M et al (2018) Ontology-based reasoning about the trustworthiness of cyber-physical systems. [arXiv:1803.07438v1](https://arxiv.org/abs/1803.07438v1)
39. Soares N, Monteiro P, Duarte FJ, Machado RJ (2021) Reference models for intelligent cities: an aligned template. In: Mahmood Z (ed) developing and monitoring smart environments for intelligent cities, 28–60. Hershey, PA: IGI Global
40. Törngren M, Sellgren U (2018) Complexity challenges in development of cyber-physical systems. In: Lohstroh M, Derler P, Sirjani M (eds) Principles of modeling. Lecture Notes in Computer Science, vol 10760. Springer, Cham
41. Ahmed ZE, Kamrul H, Saeed RA, Khan S, Islam S, Akharuzzaman M, Mokhtar RA (2020) Optimizing energy consumption for cloud internet of things. *Front Phys* 8
42. Sayed Ali E, Hasan MK, Hassan R, Saeed RA, Hassan MB, Islam S, Nafi NS, Bevinakoppa S (2021) Machine learning technologies for secure vehicular communication on internet of vehicles: recent advances and applications. *Wiley-Hindawi, Journal of security and communication networks (SCN)*, Volume 2021
43. Keramidas G, Voros N, Hübner M (2017) Components and services for IoT platforms. Paving the way for IoT standards. Switzerland Springer, Cham
44. Castaño F, Strzelczak S, Villalonga A, Haber RE, Kossakowska J (2019) sensor reliability in cyber-physical systems using internet-of-things data: a review and case study. *Remote Sens*
45. De S, Zhou Y, Abad IL, Moessner K (2017) Cyber-physical-social frameworks for urban BigData systems: a survey. *Appl Sci*
46. Capice G, Lorenzi F (2020) Blockchain and healthcare: opportunities and prospects for the HER. *Sustainability*
47. Chen HS, Jarrell JT, Carpenter KA, Cohen DS, Huang X (2019) Blockchain in healthcare: a patient-centered model. *Biomed J Sci Tech Res.* 20(3):15017–15022
48. Shi S, He D, Li L, Kumar N, Khan MK, Choo KR (2020) Applications of blockchain in ensuring the security and privacy of electronic health record systems: a survey. *Comput Secur*
49. Bhamare D, Zolanvari M, Erbad A, Jain R, Khan K, Meskin N (2020) Cybersecurity for industrial control systems: a survey. *Comput Secur* 89:101677
50. Mohanty SP et al (2019) PUFchain: Hardware-Assisted Blockchain for sustainable simultaneous device and data security in the internet of everything (IoE). [arXiv:1909.06496v1,14](https://arxiv.org/abs/1909.06496v1)
51. Mao M, Xiao H (2018) Blockchain-based technology for industrial control system cyber security. *Advances in Intelligent Systems research*, volume 147, International conference on network, communication, computer engineering (NCCE 2018)
52. Zhang R, Xue R, Liu L (2019) Security and privacy on Blockchain. *ACM Comput Surv1(1), Article 1 35p*
53. Flaus J-M (2019) Components of an industrial control system. In: Flaus J-M (Ed) Cybersecurity of industrial systems
54. Rawa DB, Chaudhary V, Doku R (2021) Blockchain technology: emerging applications and use cases for secure and trustworthy smart systems. *J Cybersecu Priv*
55. Pajoh HH, Rashid M, Alam F, Demidenko S (2021) Multi-layer Blockchain-based security architecture for internet-of-things. *Sensors*
56. Zubaydi HD, Chong Y-W, Ko K, Hanshi SM, Karuppiah S (2019) A review on the role of Blockchain technology in the healthcare domain. *Electronics* 8:679
57. Charles T, Garrocho B et al (2021) Blockchain-based process control and monitoring architecture for vertical integration of industry 4.0. *rXiv:2007.05788v2,6*
58. Prashar D et al (2020) Blockchain-based traceability and visibility for agricultural products: a decentralized way of ensuring food safety in India. *Sustainability*
59. Zeng Z et al (2020) Blockchain technology for information security of the energy internet: fundamentals, features, strategy, and application.<https://doi.org/10.3390/en13040881>
60. Pieroni A, Scarpato N, Felli L (2020) Blockchain and IoT convergence—a systematic survey on technologies, protocols, and security. *Appl Sci* 10:6749

61. Liu Y, Zhang J, Zhan J (2020) Privacy protection for fog computing and the Internet-of-things data based on blockchain. *Cluster Comput*
62. Bao S et al (2019) Pseudonym management through Blockchain: cost-efficient privacy preservation on intelligent transportation systems. *IEEE Access* 7:80390–80403
63. Silva CM, Masini BM, Ferrari G, Thibault I (2017) A survey on infrastructure-based vehicular networks. *Mobile Inform Syst*, Article ID 6123868, 28 p
64. Arena F, Pau G (2019) an overview of vehicular communications. *Future Internet* 11:27
65. Baqer Mollah M et al (2020) Blockchain for the internet of vehicles towards intelligent transportation systems: a survey. *rXiv:2007.06022v2,3*
66. Paliwal V, Chandra S, Sharma S (2020) Blockchain technology for sustainable supply chain management: a systematic literature review and a classification framework. *Sustainability* 12:7638
67. Dileep G (2020) A survey on smart grid technologies and applications. *Renew Energy* 146:2589–2625
68. Mollah MB, Zhao J, Niyato D, Lam K-Y, Zhang X, Mohammad G, Yusuf AM, Koh L, Yang L (2019) Blockchain for future smart grid: a comprehensive survey
69. Andoni M, Robu V, Flynn D, Abram S, Geach D, Jenkins D, McCallum P, Peacock A (2019) Blockchain technology in the energy sector: a systematic review of challenges and opportunities. *Renew Sustain Energy Rev* 100:143–174
70. Mika B, Goudz A (2020) Blockchain-technology in the energy industry: blockchain as a driver of the energy revolution? With a focus on the situation in Germany. *Energy Syst*
71. Xiong G et al (2021) Building urban public traffic dynamic network based on CPSS: an integrated approach of big data and AI. *Appl Sci*
72. Musleh AS, Yao G, Muyeen SM (2019) Blockchain applications in smart grid-review and frameworks. *IEEE Access* 7:86746–86757
73. Shrestha R, Bajracharya R, Nam SY (2018) Challenges of future VANET and cloud-based approaches. *Wirel Commun Mobile Comput*, Article ID 5603518, 15 p
74. Omprakash et al (2016) Internet of vehicles: motivation, layered architecture, network model, challenges, and future aspects. *IEEE Access*
75. Raza Sherazi HH, Khan ZA, Iqbal R, Rizwan S, Imran MA, Awan K (2019) A heterogeneous IoV architecture for data forwarding in vehicle to infrastructure communication. *Mobile Inform Syst*, Article ID 3101276, 12 p
76. Rafigue W, Qi L, Yaqoob I, Imran M, Rasool RU, Dou W (2020) Complementing IoT services through software defined networking and edge computing: a comprehensive survey. *IEEE Commun Surv Tutor* 22(3): 1761–1804, third quarter
77. Ahmed E, Gharavi H (2018) Cooperative vehicular networking: a survey. *IEEE Trans Intell Transp Syst*
78. Khan AS et al (2019) Secure trust-based Blockchain architecture to prevent attacks in VANET. *Sensors*
79. Mendiboure L, Chalouf M, Krief F (2020) Survey on Blockchain-based applications on internet of vehicles. *Comput Electr Eng* 84:106646.<https://doi.org/10.1016/j.compeleceng.2020>
80. Reyna A, Martín C, Chen J, Soler E, Díaz M (2018) On blockchain and its integration with IoT. *Challenges Opport Future Gener Comput Syst* 88:173–190
81. Maroufi M, Abdoolee R, Mozaffari tazekand B (2019). On the convergence of Blockchain and internetof things (IoT) technologies. *arXiv:1904.01936v1*, 11 Mar 2019
82. William et al (2020) Integration of IoT and Blockchain to in the processes of a university campus. *Sustainability*
83. Atlam HF et al (2020) A review of Blockchain in internet-of-things and AI. *Big Data Cogn Comput*
84. Hameed S, Khan FI, Hameed B (2019) Understanding security requirements and challenges in internet-of-things (IoT): a review. *J Comput Netw Commun*, Article ID 9629381, 14 p
85. Bansal S, Kumar D (2020) IoT Ecosystem: a survey on devices, gateways, operating systems, middleware, and communication. *Int J Wirel Inf Netw* 27:340–364

86. Maple C (2017) Security and privacy in the Internet-of-things. *J Cyber Policy* 2(2):155–184
87. Samaila MG, Neto M, Fernandes DAB, Freire MM, Inácio PRM (2018) challenges of securing internet-of-things devices: a survey. *Secur Priv*
88. Zhang J, Wu M (2020). Blockchain use in IoT for privacy-preserving anti-pandemic home quarantine. *Electronics* 9:1746<https://doi.org/10.3390/electronics9101746>
89. Célio et al (2021) IoT registration and authentication in smart city applications with Blockchain. *Sensors*
90. Hassan MB, Sayed Ali E, Saeed RA (2021) Intelligent Internet of things in wireless networks; Book chapter 6, edited by Mastorakis G, Mavromoustakis CX, Batalla JM, Pallis E, Intelligent wireless communications, IET book publisher, Chapter DOI: https://doi.org/10.1049/PBTE094E_ch6, e-ISBN: 9781839530968, pp 135–162
91. Hassan MB, Sayed Ali E, Nurelmadina N, Saeed RA (2021) Artificial Intelligence in IoT and its applications; Book chapter 2, edited by Mastorakis G, Mavromoustakis CX, Batalla JM, Pallis E, Intelligent wireless communications, IET book publisher, Chapter DOI: https://doi.org/10.1049/PBTE094E_ch2, e-ISBN: 9781839530968, pp 33–58
92. Alatabani LE, Ali ES, Saeed RA (2021) Deep learning approaches for IoV applications and services. In: Magaia N, Mastorakis G, Mavromoustakis C, Pallis E, Markakis EK (eds) intelligent technologies for internet of vehicles. *internet of things (Technology, Communications, and Computing)*. Springer, Cham
93. Ali ES, Hassan MB, Saeed RA (2021) Machine learning technologies on internet of vehicles. In: Magaia N, Mastorakis G, Mavromoustakis C, Pallis E, Markakis EK (eds) *Intelligent technologies for internet of vehicles. internet of things (Technology, Communications, and Computing)*. Springer, Cham
94. Jabbar S, Lloyd H, Hammoudeh M et al (2020) Blockchain-enabled supply chain: analysis, challenges, and future directions. *Multimedia Syst*
95. Nguyen C, Dinh, Pathirana P, Ding M, Seneviratne A (2019) Integration of Blockchain and cloud of things: architecture, applications and challenges
96. Fernández-Caramés T, Fraga-Lamas P (2018) A review on the use of Blockchain for the internet-of-things. *IEEE Access*
97. Schär F (2020) Blockchain forks: a formal classification framework and persistency analysis
98. Yurtseven E et al (2020) A survey of autonomous driving: common practices and emerging technologies. [arXiv:1906](https://arxiv.org/abs/1906.00001)
99. Zhou L, Liao M, Yuan C, Zhang H (2017) Low-Rate DDoS attack detection using expectation of packet size. *Secur Commun Netw*, Article ID 3691629, 14 p
100. Sayeed S, Marco-Gisbert H (2019) Assessing Blockchain consensus and Security Mechanisms against the 51% Attack. *Appl Sci*
101. Saad M, Spaulding J, Njilla L, Kamhoua C, Nyang D, Mohaisen D (2019) Overview of attack surfaces in Blockchain. In: book: *Blockchain for distributed systems security*, , pp 51–66
102. Strebko J, Romanovs A (2018) The Advantages and disadvantages of the Blockchain technology. Conference: 2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE), 1–6.<https://doi.org/10.1109/AIEEE.2018>
103. Monrat AA, Schelén O, Andersson K (2019) Survey of Blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, 1. 10.1109
104. Choi D et al (2020) Factors Affecting organizations' resistance to the adoption of Blockchain technology in supply networks. *Sustainability*
105. Choi D, Chung CY, Seyha T, Young J (2020) Factors affecting organizations' resistance to the adoption of Blockchain technology in supply networks. *Sustainability*
106. Dobrovnik M, Herold D, Fürst E, Kummer S (2018). Blockchain for and in logistics: what to adopt and where to start. *Logistics*
107. Chang V, Baudier P, Zhang H, Xu Q, Zhang J, Arami M (2020) How Blockchain can impact financial services—the overview, challenges, and recommendations from expert interviewees. *Technol Forecast Soc Change*
108. Casino F, Dasaklis TK, Patsakis C (2019) A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics Inform* 36:55–81

Blockchain in IoT and Beyond: Case Studies on Interoperability and Privacy



Abhik Banerjee , Bhaskar Dutta , Tamoghna Mandal ,
Rajdeep Chakraborty , and Rituparna Mondal

Abstract Since the boom of 2009 sparked by Bitcoin, blockchain has hardly left any field untouched. Blockchain has been countered by the lack of interoperability between different protocols. Privacy and identity management in the distributed ledger technologies have immense potential. These two areas of blockchain have seen steady progress and innovation. In this chapter, we start by first discussing recent works of blockchain and allied technologies in the field of IoT with a focus on how such works can serve as a basis for the next generation of amalgamated solutions. We give a short survey of blockchain in IoT and IIoT followed by proof of concepts of distributed ledger technology used in literature. Then this chapter gives a discussion on distributed identity management with zero knowledge proof followed by self-sovereign identity. Then we move forward with the detailed case study of Hyperledger Indy. Finally, we give case study, interoperability issue, and contemporary survey of Polkadot.

Keywords Blockchain interoperability · Polkadot protocol · Decentralized identifiers · Zero knowledge proof · Hyperledger indy · Quantum resilient Blockchain

Authors have no conflict of interest for this publication.

A. Banerjee · R. Chakraborty ()

Department of Computer Science and Engineering, Netaji Subhash Engineering College,
Kolkata, India

B. Dutta

Department of Computer Science and Engineering, University of Calcutta, Kolkata, India

T. Mandal

Department of Computer Science and Engineering, National Institute of Technology (NIT)
Durgapur, Durgapur, West Bengal, India

R. Mondal

Department of Computer Applications, Narula Institute of Technology, Kolkata, India

1 Introduction

Since its inception, blockchain emerged as a disruptive and distributed technology for the IoT industry as introduced by the Bitcoin Whitepaper and its subsequent proven application. Blockchain is regarded as a subset of Distributed Ledger Technologies [1]. However, at present, the terms “blockchain” and “distributed ledger technology” are often interchangeably used. Blockchain has hardly left any field untouched.

This chapter, thus, acts as a primer for blockchain and allied technologies being used for privacy preservation [2] and identity management [3] and presents current blockchain engines geared towards ledger interoperability. We start by discussing self-sovereign identity [4], Decentralized Identifiers (DID) [5], and Zero-Knowledge Proof [6]—three cornerstones of blockchain-based privacy preservation platforms [7] along with mentioning recent works related to the aforementioned terms. We then present two case studies. First, we review the Polkadot protocol [8], which has seen a rise at the time of writing due to its ability to facilitate cross-platform distributed ledger operations. We also present the overviews on other similar platforms dedicated to interoperability such as Cosmos and Ark. As a second case study, we discuss the Sovrin Network—pioneers of DIDs and self-sovereign identity. We also review the open-sourced framework Hyperledger Indy [9], which helps in building similar networks for identity management [10]. The latter is open-sourced by the Sovrin Foundation itself and currently hosted at the Linux Foundation under active status. Given that we are already in the NISQ-era of Quantum Computing where a substantial amount of work is being done on proposing novel applications of near-term noisy quantum, blockchain has come under scrutiny due to its reliance on cryptographic protocols deemed to be surpassable. For instance, RSA—one of the staples in encryption of communication can be broken courtesy of Shor’s Algorithm in quantum computing. While this is not an immediate possibility, it still exists as an eventuality. For this reason, recent trends indicate research being done on improving the existing blockchain and distributed ledger technology platform. The chapter, thus, concludes with a discussion of the recent works in making distributed ledger technologies robust and quantum-resilient in terms of consensus and overall architecture.

In this chapter, we first give a survey on blockchain in Internet of Things (IoT) [11] and Industrial Internet of Things (IIoT) [12], which is in Sect. 2. Section 3 describes blockchain used for identity management using zero knowledge proof, decentralized identity, and others. It also presents a case study on Hyperledger Indy—a Distributed Ledger Framework that uses ZKPs and DIDs to facilitate secure identity with selective disclosure. Section 4 describes blockchain and interoperability using the case study of Polkadot and contemporary survey of other popular interoperability solutions, which exist at the time of writing. Section 5 describes some of the open challenges, and we conclude the chapter in Sect. 6.

2 Survey on Blockchain in IoT and IIoT

Blockchain is now intensively used for IoT and IIoT. Section 2.1 gives an introduction to IoT and IIoT followed by Sect. 2.2, which gives the survey of blockchain on recent work and also proof of concepts of Distributed Ledger Technology (DLT) [13].

2.1 IoT and Industrial IoT

The Internet of Things (IoT) is the interconnection of devices and systems used to connect and communicate over the Internet. Sensors, devices, connectivity, data processing, and the user interface make the IoT the technology for the future.

Industrial IoT(IIoT) [14] is a subset of IoT. IIoT as the name suggests is generally used for the industrial sectors and applications. The use of artificial intelligence, machine learning, big data analytics, distributed system, cyber-physical systems has made the IIoT technologies [15], a boon with a reduction in human error and labor, an increase in efficiency, and a reduction of costs.

However, the possibility of cyber-attacks [16] and breach of security and privacy [17] is common in IoT [18]. This is more devastating in the case of IIoT. There are challenges in interoperability, [19] privacy, and security. The use of blockchain technologies may be the solution to overcome this problem in IoT and IIoT.

Figure 1 gives an architectural diagram, and in broad sense, IoT has four-layered architecture as below:

Sensing Layer: The IoT is basically useful for this layer. This layer consists of hardware components, which collects real-time data from the environment. These have hardware like camera, various types of sensors (temperature, motions etc.), GPS, microphone, and many more.

Network Layer: The data collected by sensors must be transferred to computing devices. This layer basically uses the existing network to transfer these data.

Data Processing Layer: These are the computers that receive the data and process it to generate information.

Application Layer: This layer uses the information generated by data processing layer and represents it to user, for example traffic conditions of a route.

Figure 2 gives the basic architecture of IIOT. IIoT basically consists of IoT, Cloud, and Edge computing facility for industrial requirements. IIoT consists of data sources as collected by sensors then these data are processed in edge layer, the next layer of IIoT. As industry requires a huge collection of data so cloud gateway comes in the next layer, and finally, execution and integration are being done in industry or factory using IIoT.

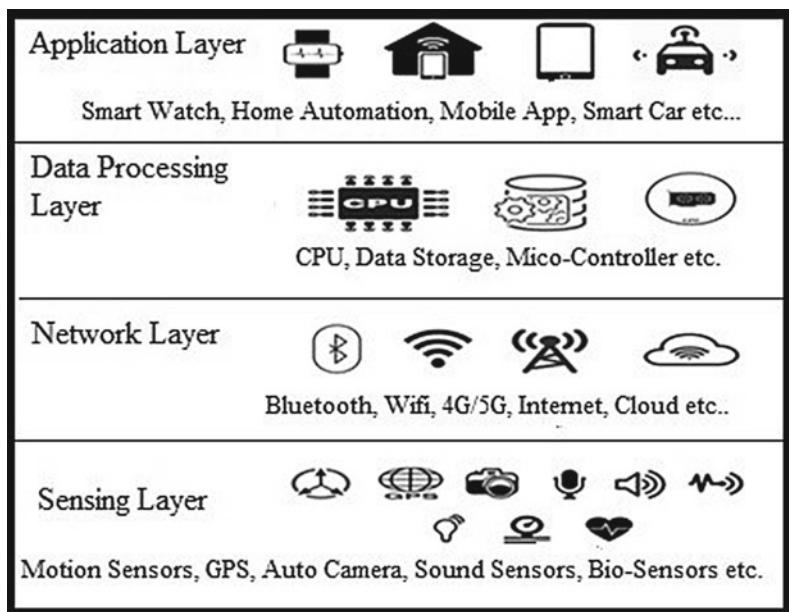
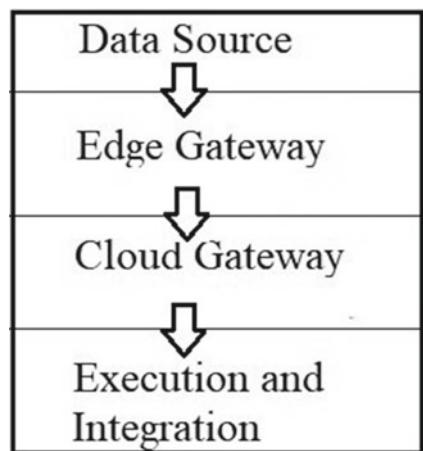


Fig. 1 IoT architecture

Fig. 2 IIoT basic architecture



2.2 Survey of Recent Works and Proof of Concepts of Distributed Ledger Technology

Two categories are there for healthcare industry in IoT, which are clinical-based services and support functional operations. IoT is helping to improve the clinical side of remote patient monitoring, or RPM. RPM is a feature that is a compelling

challenge in blockchain for IoT use cases in healthcare. Also, wearable IoT devices are being used for clinical trials by tracking all the vital signs and data among some indicators such as blood sugar, blood pressure, heart rate, weight, and others. Also, more secure remote patient monitoring is needed in medical IoT devices, and also in the drug supply chain, the other use case. In 2018, Swiss Post launched a program, which uses blockchain and integrated with IoT that tracks the temperature stability of pharmaceuticals products that are shipped in the mail. The carrier ensures that temperature-sensitive drugs such as insulin remain within an acceptable range of temperature on its journey towards patients. Blockchain technology allows Swiss Post to track these data and also share it with insurers and customers.

The next prospect of blockchain and transportation management is very important for the logistics industry that is reported by the Internet of Things Institute. Blockchain technology works with IoT-based systems in various applications likely to provide shipment data, catalog information, and blockchain also guarantees information accuracy.

Most of other issues that are access control mechanism, time required to fetch the data from different devices addressed. The centralized mechanism may have a single point of failure along with the computational overhead. So, the need for an efficient decentralized access control mechanism arises for device-to-device (D2D) communication in industrial sectors. It has been observed that blockchain can change and revolutionize most of the current and future industrial applications and also in different sectors by providing fine-grained access control.

Blockchain technologies also significantly upgrade defense mechanisms that are used in critical infrastructure protection where intrusion detection, malwares, and more specifically that of collaborative intrusion detection. IoT, thus, can transform the industry in almost every facet of applications from logistics to production to distribution. Defense Forces in India are already using a lot of IT infrastructure and applications. Strategic, tactical, operational, and logistic applications are already using a lot of IT-enabled solutions with blockchain technology.

3 Blockchain and Identity: Concepts and Case Study

Identity management is one of the challenges in the IoT environment. Section 3.1 gives the role of identity management on DLT in IoT. Section 3.2 gives some concepts related to identity management. Section 3.3 discusses Hyperledger Indy in detail.

3.1 Role of Identity Management on Distributed Ledger Technology in Internet of Things

Identity is document- or paper-based, which is prone to theft, loss, and fraud [20]. Digital identity allows us to access easily and swiftly between departments and organizations. But it has an increasing risk of being hacked, compromised, leaked or breached from the stored centralized server. So being digital is not enough. Digital identities need to be private and secure.

3.2 Concepts Relating to Identity Management

Identity management can be done using zero knowledge proof, which is described in Sect. 3.2.1, thus leading to decentralized identity management, which is described in Sects. 3.2.2 and 3.2.3 discusses another important concept known as self-sovereign identity.

3.2.1 Zero Knowledge Proof

Zero knowledge proof (ZKP) is the technique to enable data to be verified without exposing the data. Therefore, ZKP has the power to control how the data is gathered, processed, transacted, and shared. It uses a “verifier” and a “prover”. During the transaction using ZKP, the prover attempts to prove something to the verifier without informing the verifier of anything else about the thing.

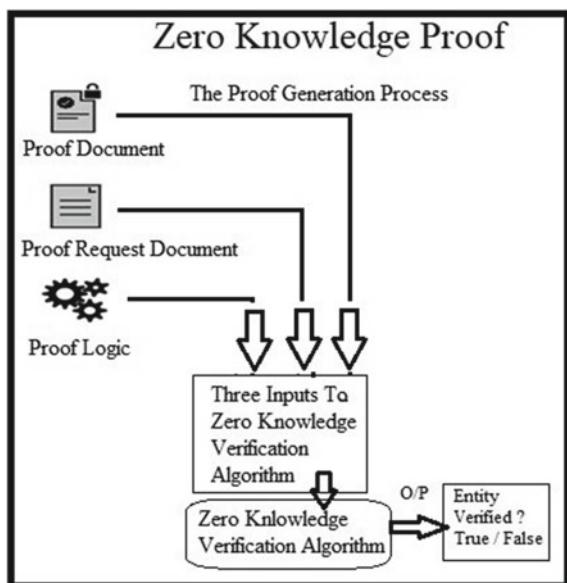
ZKP must maintain three main properties:

- Completeness:** When the statement is true, the honest verifier must ensure it by an honest prover.
- Soundness:** If the statement is false, the dishonest prover cannot prove it true to an honest verifier besides some small chance of error.
- Zero-Knowledge:** If the statement is true, no verifier will know anything about it other than the fact that it is true.

Integrating the zero knowledge proof in blockchain-based IoT will pave the path towards better interoperability [21], identity management, authentication, security [22], and privacy [23].

Figure 3 shows the basic diagram of zero knowledge proof (ZKP) [24]. The zero knowledge proof [25] is a method of identifying legitimate user without revealing the identity of the user. The ZKF consists of three parts, first is ticket generator, second is user and third is verifier, for example, if we go to movie or cinema hall we purchase ticket. So, the counter is ticket generator, while purchasing ticket here we generally don't reveal our identity such as name, address or social security number. The allowed to enter movie hall or cinema hall when this ticket is verified in the gate, so, this is the verifier algorithm. This chapter gives ZKF for cloud security.

Fig. 3 The Zero Knowledge Proof (ZKP)



3.2.2 Decentralized Identity

Our digital identity is linked with the application, service, and device we are involved with DIDs [26]. This makes the identity vulnerable to be misused because it is managed by some centralized authority or third-party service provider. Each individual has a privilege to a personality that they own and control.

Decentralized Identity fosters a greater level of control, trust, and security for apps, IoT devices [27] as well as service providers. Privacy can be guaranteed by means of pseudonymization [28]. So, instead of storing actual private data and information, the things that are stored in the blockchain are:

- Public Decentralized Identifiers (Public DIDs) and associated DID Descriptor Objects (DDOs) with verification keys and endpoints.
- Schemas
- Credential definitions
- Revocation registries
- Proofs of consent for data sharing

The concept of DIDs is credited to have been inspired from that of Uniform Resource Names (URN) [29] and in specific from that of UUIDs. UUIDs are unique identifiers that can be created locally. These are 128-bit values that can be used to uniquely identify an entity in a system. The format of a URN has been specified by RFC 8141 and can be commonly classified as:

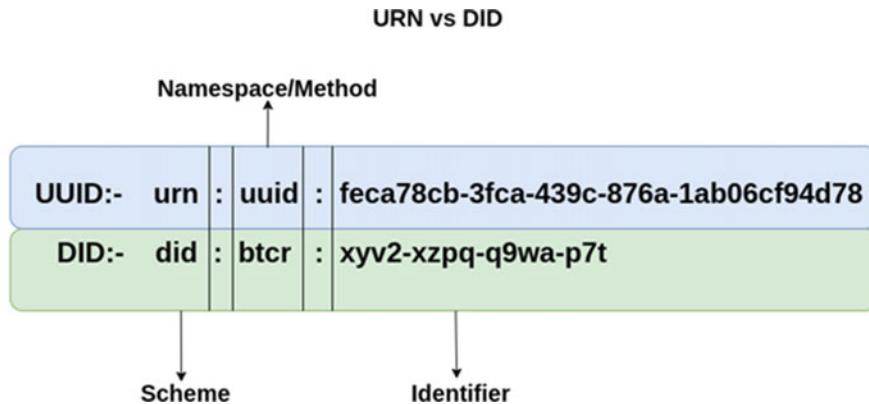


Fig. 4 URN v/s DID example

- urn: < namespace > : < identifier >

Here, the preceding characters of the first “:” indicate the scheme being used. This would be “urn” for all URN-based identifiers. The next part of the URN denotes the namespace (for example, “fruit” or “animal”). This is a common subtype to group the entities to be identified. Following the second “:” is the actual identifier of an entity (for example, “mango” or “dog”, respectively). UUIDs would have a structure as shown below:

- urn:uuid: < 128 bit identifier in hexadecimal >

When it comes to DIDs, the format remains similar except, in this case, the scheme changes, and the second part of the sequence between the colons denotes the protocol. The protocol in the case of DIDs defines the type of blockchain platform (there is a common misconception that Bitcoin is a “currency” when in fact it is the protocol that governs a token). DIDs rely on a Key Management System as well, which is cryptographically secure [30]. Figure 4 shows a common example of a DID and the basic difference between a UUID and a DID.

In Table 1, we mention some of the common decentralized identifiers under research and development by the community along with their respective designated DID prefixes. These are correct at the time of writing so please refer to their actual implementation-wise prefixes in case of a version change or community-wide adoption decision from W3C. Figure 4 illustrates an example of URN v/s DID.

3.2.3 Self-sovereign Identity (SSI)

Self-sovereign identity (SSI) is the concept where the individual has control over their identity. SSI tends to the trouble of setting up a trust in a connection. To be

Table 1 Common DID under research and development

Network/Protocol	Author	DID Prefix	Spec Hosted at
Bitcoin	Christopher Allen, Ryan Grant, Kim Hamilton Duffy	did:btcr:	https://w3c-ccg.github.io/didm-btcr/
	Jude Nelson	did:stack:	https://github.com/blockstack/blockstack-core/blob/stacks-1.0/docs/blockstack-did-spec.md
Ethereum (uPort)	uPort	did:ethr:	https://github.com/decentralized-identity/ethr-did-resolver/blob/master/doc/did-method-spec.md
Quorum	Baidu, Inc	did:ccp:	https://did.baidu.com/did-spec/
Hyperledger Fabric	SecureKey	did:trustbloc:	https://github.com/trustbloc/trustbloc-did-method/blob/master/docs/spec/trustbloc-did-method.md
	Halialabs Pte Ltd	did:emtrust:	https://github.com/Halialabs/did-spec/blob/gh-pages/readme.md
Sovrin	Mike Lodder	did:sov:	https://sovrin-foundation.github.io/sovrin/spec/did-method-spec-template.html
IPFS	TranSendX	did:ipid:	https://did-ipid.github.io/ipid-did-method/
Holochain	Holo.Host	did:holo:	https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/draft-documents/did:hc-method.md
Hedera Hashgraph	Hedera Hashgraph, Swisscom Blockchain AG	did:hedera:	https://github.com/hashgraph/did-method/blob/master/did-method-specification.md
Ledger Agnostic	DID Meme Maintainers	did:meme:	https://github.com/OR13/didme.me#did-method-spec
	Blockchain Commons	did:onion:	https://blockchaincommons.github.io/did-method-onion/
	SecureKey	did:orb:	https://trustbloc.github.io/did-method-orb/

believed, one gathering in communication will introduce certifications to different gatherings, and those depending on gatherings can check that the accreditations came from a guarantor that they trust. Table 1 gives the references of all the common DIDs, which are under research and development.

It is by and large perceived that for a character framework to act naturally sovereign, clients control the unquestionable certifications that they hold, and their nod is needed to utilize those credentials. This decreases the unintended sharing of clients' very own information.

In the SSI framework, holders produce and control exceptional identifiers called decentralized identifiers. Most SSI frameworks are decentralized, where the certifications are confirmed utilizing public-key cryptography secured on a circulated ledger.

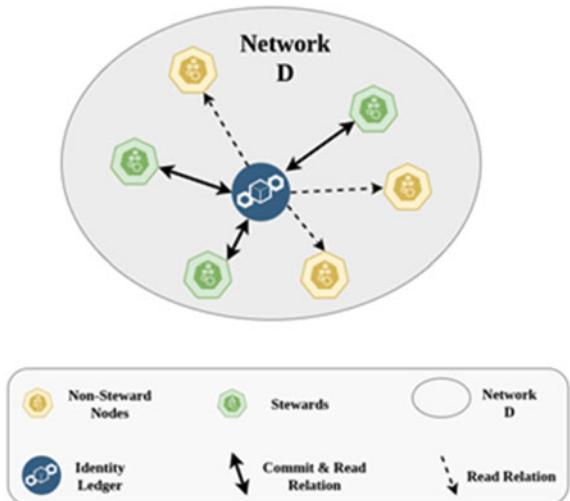
3.3 Hyperledger Indy

Hyperledger Indy is an initiative for Decentralized Identity Management. Hyperledger Indy gives tools, libraries, and reusable segments for giving computerized self-sovereign personalities established on blockchains or other disseminated records so they are interoperable across managerial spaces and applications. Initially, the Hyperledger Indy Codebase was built by Evernym. It was then donated to the Sovrin Foundation, which implemented a practical hosted ledger of identity. Indy was eventually donated and hosted at Hyperledger where it currently sits in an active status and is one of the many projects to have crossed the incubation stage at the time of writing. The advantage of using Hyperledger Indy is as follows:

- a. Users have full control over their identities.
- b. Other third parties need permission from the user.
- c. Users can utilize their identities on any network, which allows them.
- d. Users can wipe out or update ID.
- e. The user is independent on the decentralized platform.
- f. Disclosure of any documentation is limited.

In the following sections, we discuss Hyperledger Indy in detail. This is not supposed to be a full hand-on primer but rather an overview of essential concepts, which are key to developing solutions using Hyperledger Indy. For this, we propose a hypothetical network of Internet of Things Drone Network, which can be used for Surveillance. We discuss the core concepts and procedures of Hyperledger Indy using this network, which we shall, from here on out, refer to as Network D (for “Drones”). The Ledger maintained by this network D is public, and permissioned meaning anyone can view the Drones part of the network and the transactions but not commit/write to the ledger in any fashion.

Section 3.3.1 discusses core concepts of Hyperledger Indy, Sect. 3.3.2 gives the onboarding process for a drone [31] (entry into the network), Sect. 3.3.3 outlines revocation of entry, and Sect. 3.3.4 gives active use cases of Hyperledger Indy.

Fig. 5 The Stewards

3.3.1 Core Concepts

This section discusses the core concepts of a Hyperledger Indy Network along with the consensus protocol used by it. It also serves the example of Network D while explaining the procedures relating to the network. The core concepts are explained from Sects. 3.3.1.1–3.3.1.8.

Stewards

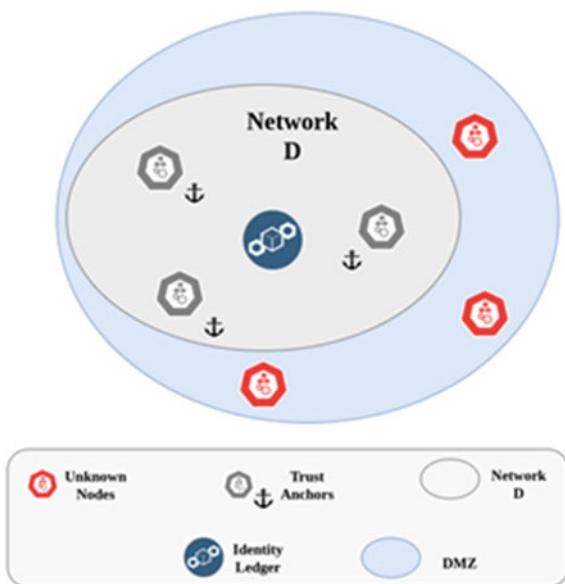
Indy is intended to be worked to such an extent that everybody can see the substance of the blockchain, however, just pre-endorsed members, known as Stewards, are allowed to take part in the approval interaction.

Stewards can compose the exchange into the Hyperledger Indy record kept up by Sovrin. Stewards can be a prominent government-claimed organization whose errand is to run and keep up the Sovrin network. To turn into a Steward, there is an appropriate onboarding measure characterized by Sovrin. Figure 5 shows the block diagram of Steards.

Trust Anchor (TA)

Indy Stewards are nodes of the Hyperledger Indy network that have authorizations to take an interest in the approval interaction. Trust Anchor is the connection between User and Stewards. TA can be banks, colleges, medical clinics, specialist co-ops, protection companies. TA acknowledges the solicitation from the client and advances

Fig. 6 Actors in Hyperledger Indy



this solicitation to Stewards if there should arise an occurrence of composing into the ledger record.

Figure 6 shows the concept of Trust Anchor where the Drones already a part of the Network D are depicted as Grey Trust Anchors while the outside newly booted drones or hostile drones are not trusted. The Grey space denotes Network D, which is depicted as a part of the Demilitarized Zone or the Digital Space or Internet. It may be noted here that the diagram shows a centralized ledger for storing Identity. This is not the case and it has been depicted so due to ease of representation. The following concepts on Ledger and Pool Nodes will clarify this as a decentralized record ledger maintained by nodes in the network.

Verinym, Pseudonym and Pairwise Unique Identifiers

The Decentralized Identities (DIDs) are of two sorts. The first is a Verinym. Verinyms are DIDs that are approved to be kept in touch with the Sovrin Ledger utilizing the advanced mark of a Trust Anchor so they might be straightforwardly or in a roundabout way connected with the Legal Identity of the Identity Owner. Verinyms are required for the lawful responsibility of Trust Anchors. It is related to the Legal Identity of the Identity Owner. For instance, all gatherings ought to have the option to check that some DID is utilized by a government to distribute diagrams for some record types.

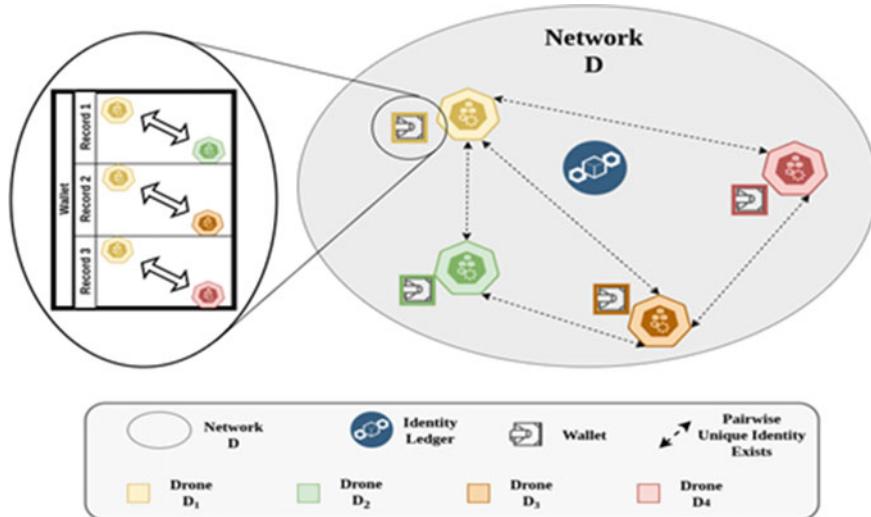


Fig. 7 The nodes

The subsequent kind is a Pseudonym—a Blinded Identifier used to keep up security with regard to a progressing advanced connection. In the event that the Pseudonym is utilized to keep up just a single relationship, we will consider it a Pairwise-Unique Identifier.

Note the relation of Pairwise Unique Identifiers is explained in Fig. 7, the wallet section where Drone D₁ has Pairwise DID with Drones D₂, D₃, D₄ but Drone D₂ on the other hand shares a DID with Drones D₁ and D₃ only. In the same diagram, it is apparent that Drone D₄ has made communication with Drones D₁ and D₃ during its lifetime in the Network D and so is unaware of Drone D₂.

Wallet

The wallet is the secure capacity for cryptographic tools like DIDs, keys, and so on. It is an advanced compartment for information that is expected to control a self-sovereign identity. A common misconception is that Identity Wallet is the same as cryptocurrency wallets. However, an identity wallet can hold something beyond cryptographic money keys. Wallets may have to oversee many relationships.

In Fig. 7, we show the concept of wallets where the pairwise unique identifiers or DIDs are stored in records. Every wallet is private to its drone and only stores the record of any other drone, which may have initiated any form of communication with it. In doing so, the communicating drone must have had to identify itself by establishing a common truth and proving its identity through the shared identity ledger. This would mean it generated a pairwise unique identifier with the drone it was communicating with.

At this point, it should be clear how the concept of SSI, DID and Wallets gives an identity to an entity in the network. This identity is not federated and hence cannot be taken away when a third party stops functioning. Thus, it also removes the risk of data leakage on part of the third party. The aforementioned two points are considered to be two gaping disadvantages of Federated Identity (a common example would include signing up or logging into a site using one's Gmail, Facebook, or GitHub ID).

It also removes the risk of correlation of identities of an entity to a great extent since these identities are “pairwise” unique. Consider a case where a subject repetitively uses his or her Facebook to log into multiple sites. These sites may or may not share data among themselves. But if two or more of these sites get breached and the data of the user is stolen, it would be easy to correlate the data from multiple sites and link it to a person since the data contain common elements from the Facebook Login.

Nodes (Validators, Observers)

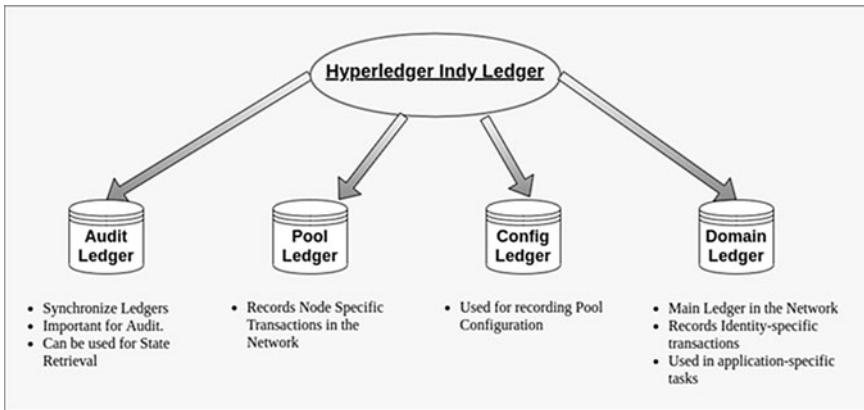
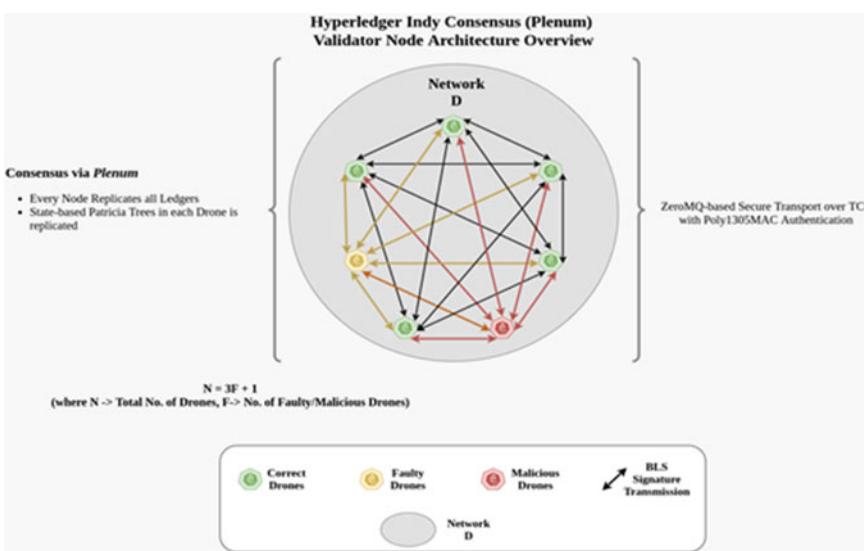
The important feature in Hyperledger Indy is that it is public yet permissioned ledger. The main architecture of it comprises Validators and Observers. These are regarded as Nodes in the network. A node can be anything ranging from a server, to a virtual machine or a docker container running in a Kubernetes Pod. Validator Pool handles Writes and Reads. These nodes participate in consensus. On the other hand, Observer Pool handles Reads. Observers keep their states synchronized with the Validators. Figure 7 illustrates the nodes acting in the network.

Ledger

Ledger is an ordered log of transactions stored in a DLT network. This is basically the core of the whole “Blockchain” or “Distributed Ledger” ideology. Ledgers are basically databases that are replicated across nodes in a network. Indy has different types of ledgers each with a separate transaction log and merkle tree. Figure 8 shows the ledgers available in Hyperledger Indy.

Redundant Byzantine Fault Tolerance and Plenum

Redundant Byzantine Fault Tolerance or RBFT is a variant developed from Practical Byzantine Fault Tolerance consensus mechanism. It works on the concept of “multi-phase commit” for reaching consensus on a specific piece of information (hence the “Redundant”). Plenum is Hyperledger Indy’s implementation of RBFT and works at the core of the Indy Nodes to provide secure consensus. Because of it, Indy Nodes’ Network can tolerate a 33% failure rate (including malicious actors and malfunctioning actors). Figure 9 gives the consensus, Plenum.

**Fig. 8** Ledgers in HI**Fig. 9** Consensus in HI

Credentials

An undeniable credential gives a standard method to carefully communicate qualifications in a manner that is cryptographically secure, privacy respecting. An element called an issuer produces and signs such accreditations with its private key. A verifier can look into the public key of a given DID, related to a given certification on a certain information library.

A Credential Definition can be made and saved in the Ledger by any Trust Anchor. By and large, the issuer offers a credential. Then, the holder demands the credential, providing the blinded connection secret that will tie it to them. At long last, the issuer creates the accreditation and offers it to the holder.

3.3.2 Onboarding Process for a Drone (Entry into the Network)

The onboarding process is what new drones (say D_x) go through before joining Network D, shown in Fig. 10. This is also the part where the presence of SSI through DID shines. As mentioned earlier, SSI or self-sovereign identity allows for partial disclosure without compromising trust. This means that details like a drone's company or its manufacturing technology can be kept under wraps even if it joins the Network D. In our example, let's assume that there is a composite network of drones from various manufacturers, and these drones are commissioned by an Entity "ABC" (this may be a Government Consortium in a real-world scenario or a single individual). There are drones bought from three different companies—DJI (Dajiang) Innovations, Ambarella, and Boeing (at the time of writing these are touted as three of the biggest names in this field by Business Insider [31]). Network D is, thus, a composite of different types of drones from different manufacturers wishing to prevent technology theft on their part. Figure 10 shows the start of the onboarding of a New Drone D_x made by Boeing into Network D.

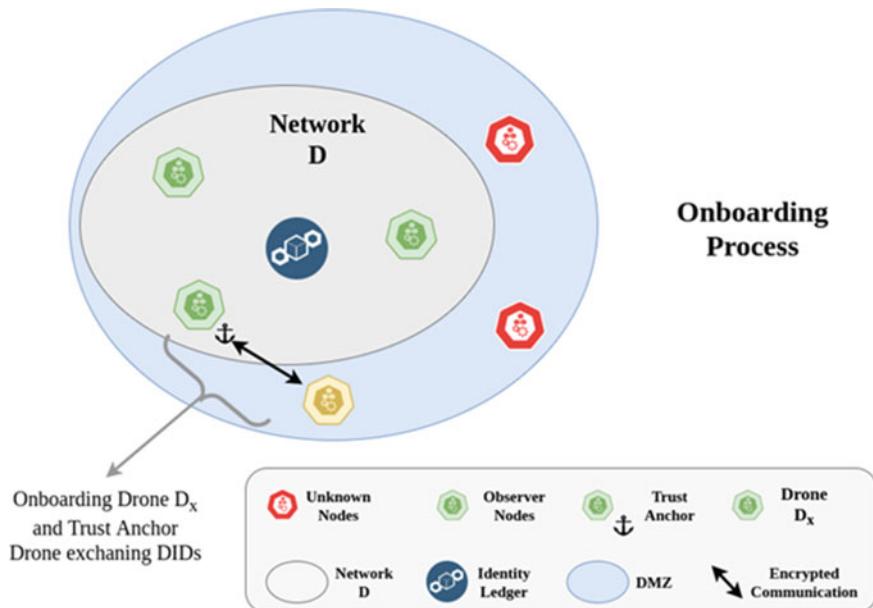


Fig. 10 The onboarding process of drones

The following list of steps is followed by Drone D_x and one Drone already in the Network D, which functions as a Trust Anchor:

1. Drone D_x , which has received a mark of approval from ABC, pings the Network D to find the IP of a Trust Anchor and then pings the Trust Anchor signaling it wants to initiate the onboarding process.
2. The Drone acting as the Trust Anchor now creates a DID Record in the Wallet that it will use for securely communicating with Drone D_x and then builds an NYM request to the ledger for recording.
3. The Trust Anchor initiates a connection request to the Drone D_x sending the DID along with a cryptographical challenge for it to solve. For ease of understanding, we will assume that the challenge is a Nonce of “A123F234” (hexadecimal sequence), which Drone D_x needs to include in its reply back to the Trust Anchor. This Nonce can be used only once.
4. Drone D_x accepts the requests. It then creates its wallet and creates a DID and its respective Verification Key, which it will use for communication with the Trust Anchor Drone. In the connection response, Drone D_x includes the approval from ABC, DID for Trust Anchor which it had made, the Nonce “A123F234”.
5. Drone D_x then queries the Ledger for verkey of the DID that was sent to it by the Trust Anchor Drone (recall the Network D Ledger is public and permissioned). Since DIDs are pairwise unique, this DID can only be used between Drone D_x and the Trust Anchor inside the Network D.
6. The connection response is now encrypted anonymously (Indy provides a crypto.anon_crypt API for this). The Trust Anchor inside the Network can use its private key to decrypt this response and can validate its integrity. Drone D_x sends this response.
7. Trust Anchor Drone inside the Network receives this response. It decrypts the response by using the crypto.anon_decrypt API provided by Indy and validates it by checking the approval from ABC (which should match with its own approval), the Nonce from the response.
8. The Trust Anchor now sends the DID received from Drone D_x to the Ledger as an NYM Transaction. While it is sent by the Trust Anchor, ownership of it belongs to Drone D_x . This creates a trusted connection between the two.

This completes the first stage of the process. In the next stage of the onboarding process, Drone D_x uses the record of its DID with the Trust Anchor Drone to create a DID for itself stating its identity. This kind of DID is termed as Verinym. This DID is sent back to the Trust Anchor who again commits it to the ledger. This particular communication between the two is encrypted using the Sender and Receiver's private and verification keys, respectively, using crypto.auth_crypt API from Indy. This is reversible at the receiver's end. The Receiver decrypts it using the crypto.auth_crypt API. This completes the whole process. Drone D_x is now a part of Network D.

3.3.3 Revocation of Entry

The membership of an entity in a blockchain network is dependable on its reputation. Network D is no exception. To revoke the membership all that needs to be done is put in a Revocation record in the Ledger. This too can be easily done using the `build_revoc_reg_entry_request` and `sign_and_submit_request` Ledger APIs from Hyperledger Indy at the time of writing.

3.4 Active Use Cases of Hyperledger Indy

The three active use cases are:

- a. **Kiva's** launch of Africa's first national decentralized ID system with Hyperledger Indy: Kiva, a US charitable association centered with respect to monetary consideration has constructed Kiva Protocol to help empower widespread monetary access. In 2019, Sierra Leone, a West African country of around 7 million, dispatched the National Digital Identity Platform (NDIP) that utilized Kiva Protocol to empower quick, modest, and secure character check for its residents. It allows citizens to perform electronic Know Your Customer (eKYC) verifications in about 11 s, using just their national ID number and a fingerprint.
- b. **CULedger** protects credit unions against fraud with Hyperledger Indy: CULedger worked with decentralized personality association, Evernym, to fabricate a recognizable proof arrangement that was quicker, less complex, and safer with Hyperledger Indy—a dispersed record programming project that is interoperable with other blockchains or can be utilized all alone to control the decentralization of identity. It has brought the interoperability and portability to scale towards a newer height.
- c. **The Verifiable Organizations Network (VON)**, started by the governments of British Columbia, Ontario, and Canada, aims to cut government red tape with Hyperledger Indy.

Hyperledger Indy use cases can be found in the areas of digital documentation, password-less authentication, software vulnerability attack, tackling spam, document provenance, education and employment verification, decentralized membership management, and global accessibility.

The entire digital identity community is looking forward to Hyperledger Indy for a safe, secure, and serene future. There is a huge chance to succeed.

4 Blockchain and Interoperability: Case Study of Polkadot and Contemporary Survey

In this section, we will discuss Blockchain and Interoperability issues in IoT with a case study and survey. Section 4.1 describes the Role of Blockchain Interoperability [32] in IoT, Sect. 4.2 gives a case study on Polkadot protocol, and finally, Sect. 4.3 gives a survey of contemporary interoperability Engines and Platforms.

4.1 *Role of Blockchain Interoperability in IoT*

Given that every day new developments are done in the field of blockchain and IoT and soon they will be implemented side by side. Based on the requirements and use case, different IoT projects can have their own blockchain network with different networks interacting with each other as and when needed. For example, the Traffic Lights can have their own blockchain network with a specific consensus mechanism and smart cars have their own blockchain with a suitable consensus mechanism. These two networks can interact with each other to fetch data or perform operations when needed like when cars follow the traffic light, tokens are issued for the smart car.

In our previous case study of Hyperledger Indy, we used the example of Network D consisting of drones manufactured by three different entities but being operated in the same network by an entity “ABC”. Consider a scenario where this identity-based ledger solution needs to interoperate with another distributed ledger solution like malicious activity detection. This specific DLT can be implemented using a different framework than Hyperledger Indy (since Indy only specializes in Identity). It can be a R3 Corda network or a Hyperledger Fabric one for example. However, for accurate functioning, that specific network needs to interact with Network D for a trustable proof of identity between communicating drones. If a drone has detected a person where there should be none then it may need to relay that information to other drones in the Network as well as record it in the ledger being used to record suspicious activities. Here, we can see the need for a common ground when the IoT devices, i.e., the drones in Network D want to relay information across different blockchain types. This is where the phenomenon of Blockchain Interoperability comes into play. The two networks made from two very different frameworks might not operate in a compatible manner. This can be the result of different formats of API responses, node architecture, or secure connection algorithms used.

For this reason, it is common to use another blockchain or interoperability engine like an OS for making sure that transactions from one ledger can smoothly be translated onto a different one. Polkadot is the former. It is a ledger-based solution to the problem. The following sections discuss Polkadot and its important components.

4.2 Case Study on Polkadot Protocol

As described on their official website, “Polkadot is a heterogeneous multi-chain with shared security and interoperability”. The Polkadot chain has a central main chain, known as the Relay Chain. All validators of the Polkadot network are staked on this Relay Chain, and DOT is the native cryptocurrency of this chain. It should be noted that this relay chain has limited functionalities, and smart contracts are not supported on the relay chain. The main purpose of the Relay Chain is to coordinate the system as a whole including other parachains.

When it comes to interoperability, what makes Polkadot unique is its concept of **Parachains** and **Parathreads**. Like cores on a computer’s processor, Polkadot supports execution slots that can be subscribed to. Either DOT can be staked to lease a slot (in case of Parachain) or pay on a per-block basis (in case of Parathreads).

Parachains can be considered as the separate blockchain of their own, which are connected to the Relay Chain. The parachain has its own set of validators and *Collators*. These parachains, however, can’t have their own consensus mechanism but can have their own economics and own native tokens. Parachains can interact with each other through *XMCP*.

The official wiki of Polkadot compares Parathreads with swap memory in computers. The main difference between Parachain and Parathreads being parathreads doesn’t have a dedicated slot and compete on a per-block basis. This is greatly helpful because this needs less capital, and parachain can be changed to parathread in future and vice versa. Parachains too can communicate with other parachains or parathreads through XMCP.

Figure 11 depicts Relay Chain, Parathreads, and Parachains through XMCP.

Besides parachains and parathreads, Polkadot also has the concept of *Bridges*. As the name suggests, Bridges can like connecting modules or smart contracts that help Polkadot interact with other blockchain networks like Ethereum and Bitcoin. This opens up a newer horizon of implementation because bridges can connect two blockchains that are otherwise economically sovereign and technologically unique.

The Polkadot ecosystem has two types of bridges.

- a. Bridge Module
- b. Bridge Contract

Bridge Modules are designed to receive messages from non-parachain blockchain, which are then deployed to Polkadot either as a system-level parachain or a community-operated parachain. Because of this, these non-parachain blockchains act like virtual parachains, which can then have the interoperability benefits of Polkadot.

Bridge Contract can be used to interact with blockchains, which support smart contracts like Ethereum. This is a result of two smart contracts, one in each network. Since Polkadot Relay Chain doesn’t support smart contracts, a parachain that supports smart contract must be used. These smart contracts interact with each other to achieve the goal. So, for example, depositing DOT on a smart contract in a parachain may generate some ERC20 token in the Ethereum Mainnet.

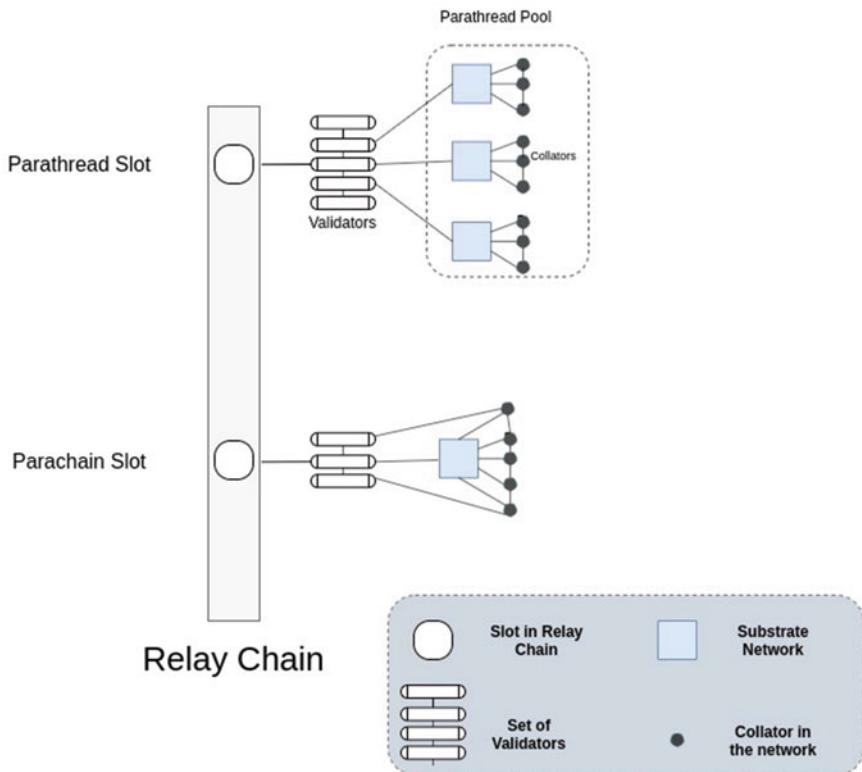


Fig. 11 Relay chain, Parathreads, and Parachains through XMCP

Now given that we understand the various methods of achieving interoperability using Polkadot, now let's discuss each of these aspects in regard to implementing it with IoT projects. The following sections discuss the usage aspects of Polkadot elements in solutions.

I. Using Parathreads

As discussed, Parachains and Parathreads form an integral part of the Polkadot ecosystem. However, each of them has some limitations. They are bound by the economic model and the technology used. But this also means easy implementation and scaling. The best use case for these can be in case of micro-payments. If the IoT system is focused on rewarding people based on certain criteria, a parathread can be used. It will be a more economic implementation and would also ensure faster transactions.

II. Using Parachain

If a separate side chain is needed to be implemented, then Parachain would be the ideal choice. A separate chain may be needed if the IoT project is focused on simultaneous

interaction of more than one smart device. The parachain can have its own set of validators and also its own cryptocurrency. It should be noted that Parachains can't implement their own consensus model and would require reserving a slot in the Relay Chain via auction using DOT.

III. Using Bridges

Under certain extreme cases, it may be necessary to implement a separate blockchain, which is technically unique. It may also be so that a certain group of smart devices, which is already running on blockchain, wants to be a part of the larger ecosystem. In such cases using Parachain may not fulfill the requirement. Under these circumstances, bridges are to be used. If the blockchain supports smart contracts that Bridge Contracts can be used for easier implementation. Otherwise, separate Bridge Modules can be designed using substrate to achieve the goal of interoperability. However, it should be noted that Bridges can't directly connect to a slot in Relay Chain and must connect via a Parachain or a Parathread.

IV. Support of Smart Contract

Substrate is the framework that is used to build polkadot, and this can be used to build other blockchains, which can interact with the Polkadot Relay Chain by any of the previous discussed methods. Substrate enables us to create blockchains, which can or cannot support smart contracts. Support of smart contract plays an important role when using blockchain for IoT and more evidently when frameworks like Substrate are used.

Supporting smart contract has the following pros when considered with respect to IoT:

1. Implement condition-based decision-making on-chain.
2. Enable future applications to be built on the blockchain.
3. Create a defi-based model coupled with the IoT implementation.

However, integrating smart contracts also has some cons associated with it:

1. The node requires more resources and most IoT projects have limited resources.
2. Smart contracts are a source of vulnerability where anyone can exploit a bug in any smart contract for personal benefits.

While creating the side chain, the above points must be considered. Since most IoT projects are inclined towards faster transactions, smart contracts can be an added overhead with limited benefits.

4.3 *Survey of Contemporary Interoperability Engines and Platforms*

When it comes to interoperability and cross-chain transaction, Polkadot is not the only one in the race. At a base level, using Oracles can help achieve some of the

needed interoperability but those are neither easy to implement nor easily scalable. Some other blockchain technologies that also aim at interoperability are *Blocknet*, *Aion Online*, *Wanchain*, *Cosmos Blockchain*.

Among all the mentioned projects, Cosmos Blockchain is one of the popular options [33]. Blockchain networks built using prebuild and/or custom modules using the Cosmos SDK can interact with other Cosmos Blockchain via IBC to Cosmos Hub. IBC or Inter-Blockchain Communication Protocol is an end-to-end, connection-oriented communication protocol designed for interaction between heterogeneous blockchain networks. Using IBC, a wide range of Dapps can be built, which can facilitate tasks like cross-chain token transfer and atomic swaps. Presently, IBC is implemented using Cosmos SDK.

5 Open Challenges and Discussions

Although integrating blockchain with IoT unlocks new potentials, they are still subjected to certain challenges [34]. This section discusses two of such challenges, which have seen enormous amounts of research work in recent years but still have not been perfectly addressed.

- I. **Transaction Speed:** The throughput of the blockchain network, which is measured by the number of transactions per second, can act as a bottleneck in case of IoT. Most IoT solutions require fast decision-making and record-keeping, which demands high throughput. To achieve this, such a consensus mechanism should be introduced, which can promise high throughput without compromising security. Consensus algorithms have been proposed that “solve” this problem but each of these has its own disadvantages. For instance, Byzantine Fault Tolerance derivative algorithms have high asymptotic complexity, Proof of Stake, which was proposed as an alternative to Proof of Work introduces centralization in the system in form of prejudicial “stake” in the whole network asset, Kafka has also been tested out in Hyperledger Fabric and has seen criticism because it introduces a single point of failure in the network during consensus. As such a balance between transaction speed and the aforementioned handicapping factors does not exist in literature at the time of writing.
- II. **Running Nodes:** A blockchain network comprises multiple nodes, which are responsible for validating transactions and adding new blocks. In most cases, validating a transaction includes solving a cryptographic puzzle, which requires computing power. How the network rewards this computing power is decided by the consensus mechanism, however, the network is dependent on computers, which can solve these puzzles. This makes blockchain network resource-intensive, which makes it challenging to implement it cost-effectively and scalably in IIoT solutions. However, there are works in literature, which show a

Proof of Concept as well as Production Systems, which function with this handicap. US Defense, for instance, proposed such a system of UAV (Unmanned Aerial Vehicle) drones [35].

6 Conclusion

Thus, in this chapter, we discussed Blockchain in IoT covering one important survey on IoT and IIoT, proof of concepts of DLT. Then we move forward with issues of identity management through Blockchain in IoT and IIoT. Then we discussed blockchain and Interoperability issues in IoT with a case study of Polkadot protocol with relay chain. Two major issues, transaction speed and multiple running nodes, are also introduced in this chapter. In this chapter, we discussed transaction speed and running nodes as open challenge. Hyper Ledger Indy also been discussed with the example of onboard processing of drones. DID and SSID are also discussed with the introduction to zero knowledge proof. Therefore, we can conclude that blockchain is now effectively used in IoT for identity management, and it is very much interoperable in the current industry.

References

1. Kuchin NV, Polyakov KO, Butakova NG (2020) Transaction protection in corporate networks based on distributed ledger technology. 2020 IEEE conference of russia young researchers in electrical and electronic engineering (EIConRus), St. Petersburg and Moscow, Russia, pp 2072–2076. <https://doi.org/10.1109/EIConRus49466.2020.9039210>
2. Bernabe JB, Canovas JL, Hernandez-Ramos JL, Moreno RT, Skarmeta A (2019) Privacy-preserving solutions for Blockchain: review and challenges. In: IEEE Access. <https://doi.org/10.1109/ACCESS.2019.2950872>
3. Khovratovich D, Law J (2020) Sovrin: digital identities in the blockchain era. In: White Paper Sovrin. <https://sovrin.org/library/sovrin-digital-identities-in-the-blockchain-era/>
4. Liu Y, Lu Q, Paik H-Y, Xu X, Chen S, Zhu L (2020) Design pattern as a service for Blockchain-based self-sovereign identity. IEEE Softw. **37**(5): 30–36. <https://doi.org/10.1109/MS.2020.2992783>
5. Kim B, Shin W, Hwang D-Y, Kim K-H (2021) Attribute-based access control (ABAC) with decentralized identifier in the Blockchain-based energy transaction platform. 2021 International conference on information networking (ICOIN), Jeju Island, Korea (South), 2021, pp 845–848. <https://doi.org/10.1109/ICOIN50884.2021.9333894>
6. Harikrishnan M, Lakshmy KV (2019) Secure digital service payments using zero knowledge proof in distributed network. 2019 5th international conference on advanced computing & communication systems (ICACCS), Coimbatore, India, 2019, pp 307–312. <https://doi.org/10.1109/ICACCS.2019.8728462>
7. Shi P, Wang H, Yang S, Chen C, Yang W (2019) Blockchain-based trusted data sharing among trusted stakeholders in IoT. Wley Publication. <https://doi.org/10.1002/spe.2739>
8. Burdges J et al (2020) Overview of Polkadot and its design considerations. In: White paper of Web3 foundation, parity technologies. <https://eprint.iacr.org/2020/641.pdf>
9. Bhattacharya MP, Zavarsky P, Butakov S (2020) Enhancing the security and privacy of self-sovereign identities on Hyperledger Indy Blockchain. 2020 international symposium on

- networks, computers and communications (ISNCC), Montreal, QC, Canada, 2020, pp 1–7. <https://doi.org/10.1109/ISNCC49221.2020.9297357>
- 10. Bhattacharya A (2021) Blockchain-based identity management. Wiley Publication. <https://doi.org/10.1002/9781119711063.ch7>
 - 11. Choudhury T, Khanna A, Toe TT, Khurana M, Nhu NG (2021) Blockchain applications in IoT ecosystem. EAI/Springer innovations in communication and computing, eBook ISBN 978-3-030-65691-1, Series ISSN 2522-8595. <https://doi.org/10.1007/978-3-030-65691-1>
 - 12. Senathipathi K, Kayalvili S, Anithaa P, Carol Henna KJ (2021) Blockchain integrated IIOT—future of IOT. In: Emerging trends in materials science, technology and engineering, Elsevier. <https://doi.org/10.1016/j.matpr.2020.12.1051>
 - 13. Hofman D et al (2018) building trust & protecting privacy: analyzing evidentiary quality in a Blockchain proof-of-concept for health research data consent management. 2018 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCoM) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp 1650–1656. https://doi.org/10.1109/Cybermatics_2018.2018.00275
 - 14. Dhirani LL, Armstrong E, Newe T (2021) Industrial IoT, cyber threats, and standards landscape: evaluation and roadmap. Sensors 21(11):3901. <https://doi.org/10.3390/s21113901>
 - 15. Choudhary K, Gaba GS, Butun I, Kumar P (2020) MAKE-IT—a lightweight mutual authentication and key exchange protocol for industrial internet of things. Sensors 20(18):5166. <https://doi.org/10.3390/s20185166>
 - 16. Zhang R, Xue R (2019) Security and privacy on Blockchain. In: ACM computing surveys, 2019 association for computing machinery, 0360–0300/2019/1-ART1. <https://doi.org/10.1145/3316481>
 - 17. Conti M, Sandeep Kumar E, Lal C, Ruj S (2018) A survey on security and privacy issues of Bitcoin. IEEE Commun Surv Tutor 20(4): 3416–3452, Fourthquarter 2018. <https://doi.org/10.1109/COMST.2018.2842460>
 - 18. Halpin H, Pieckarska M (2017) Introduction to security and privacy on the Blockchain. In: 2017 IEEE European symposium on security and privacy workshops (EuroS&PW)
 - 19. Monika, Bhatia R (2020) Interoperability solutions for Blockchain. 2020 international conference on smart technologies in computing, electrical and electronics (ICSTCEE), pp 381–385. <https://doi.org/10.1109/ICSTCEE49637.2020.9277054>
 - 20. Wilson Y, Hingnikar A (2019) Solving identity management in modern applications. Book Published by Apress, eBook ISBN 978-1-4842-5095-2. <https://doi.org/10.1007/978-1-4842-5095-2>, Softcover ISBN 978-1-4842-5094-5
 - 21. Dimitrov I, Gigov R (2020) Exploring interoperability of Blockchain technology and the possibility of collaboration with the existing information systems of the enterprises. 2020 III international conference on high technology for sustainable development (HiTech), 2020, pp 1–4. <https://doi.org/10.1109/HiTech51434.2020.9363987>
 - 22. Piscini E, Dalton D, Kehoe L (2020) Blockchain & cyber security. Let's discuss. In: White paper of Deloitte
 - 23. Henry R, Herzberg A, Kate A (2018) Blockchain access privacy: challenges and directions. In: Blockchain security and privacy, Copublished by the IEEE computer and reliability societies 1540–7993/18
 - 24. Smart NP (2016) Zero-knowledge proofs. In: Cryptography made simple. information security and cryptography. Springer, Cham. https://doi.org/10.1007/978-3-319-21936-3_21
 - 25. Fischlin M, Rohrbach F (2021) Single-to-multi-theorem transformations for non-interactive statistical zero-knowledge. In: Garay JA (eds) Public-key cryptography—PKC 2021. PKC 2021. Lecture Notes in Computer Science, vol 12711. Springer, Cham. https://doi.org/10.1007/978-3-030-75248-4_8
 - 26. Steele S(Transmute), Sporny M(Digital Bazaar) (2021) DID specification registries: the interoperability registry for decentralized identifiers. <https://www.w3.org/TR/did-spec-registries/#did-methods>

27. Buyya R, Dastjerdi AV (2016) Internet of things. Elsevier Publication, eBook ISBN: 9780128093474, Paperback ISBN: 9780128053959.
28. Shancang L, Xu LD (2017) Securing the internet of things. Elsevier publication, eBook ISBN: 9780128045053, Paperback ISBN: 9780128044582
29. Saint-Andre P et al (2017) Internet engineering task force (IETF), 8141 document on URN. <https://tools.ietf.org/html/rfc8141>
30. Barker E (2013) NIST white paper on “a framework for designing cryptographic key management systems”. <https://csrc.nist.gov/publications/detail/sp/800-130/final>
31. Drone and Drone Manufacturing Details. <https://www.businessinsider.com/drone-manufacturers-companies-invest-stocks?IR=T>
32. Belchior R, Vasconcelos A, Guerreiro S, Correia M (2020) A Survey on Blockchain interoperability: past, present, and future trends. In: 2020 association for computing machinery
33. Kwon J, Buchman E, COSMOS: a network of distributed ledgers. In: White paper of <https://cosmos.network/cosmos-whitepaper.pdf>
34. Makridakis S, Christodoulou K (2019) Blockchain: current challenges and future prospects/applications. Future Internet 11(258):1–16. <https://doi.org/10.3390-fi11120258> www.mdpi.com/journal/futureinternet
35. Ahmad R, Hasan H, Yaqoob I, Salah K, Jayaraman R, Omar M (2020) Blockchain for aerospace and defense: opportunities and open research challenges. Comput Indust Eng 151. <https://doi.org/10.1016/j.cie.2020.106982>

Hybrid Blockchain-Enabled Security in Cloud Storage Infrastructure Using ECC and AES Algorithms



Mhamad Bakro , Sukant K. Bisoy , Ashok K. Patel , and M. Adib Naal

Abstract Due to the high growth of Internet of Things and cloud computing services it has brought great changes within the human lifestyle in various fields such as (medical, agricultural, educational, military, environmental, etc.). So, it was necessary to understand the building blocks' basic of the Internet of Things and identify weaknesses and data security of user. Blockchain plays an important role in the implementation of security aspects in cloud computing. In this work, we have analyzed the security aspects of data stored in the cloud through hybrid security system enabled with blockchain technology using cryptographic algorithms ECC and AES. Our framework is having higher security with more efficiency than others.

Keywords Cloud computing · Cloud storage · Cloud security · Cryptography algorithms · Blockchain

1 Introduction

What makes the user move to the IoT and cloud or continue in the traditional system is the extent of his confidence in the service provider. This trust depends on taking the provider into account all problems such as privacy problems, information security “being corrupted or stolen data”, infrastructure security, application security, network security, identity management, authorization, service availability, service interruption in the case of cloud (as happened with Google, Amazon, and Microsoft due to server downtime due to maintenance of some of it and overloading on other servers, file leaks, electricity outages due to lightning, etc.), access control, authentication, unintended data loss, failure (and this failure may happen as a result of infrastructure devices in the cloud “IaaS layer”, or malware software “SaaS layer”,

M. Bakro · S. K. Bisoy · A. K. Patel

Department Computer Science and Engineering, C. V. Raman Global University,
Bhubaneswar 752054, India

M. A. Naal

Department Computer Science and Engineering, Kalinga Institute of Industrial Technology,
Bhubaneswar 751024, India

or as a result of malicious code or a malfunction in user applications or a third party injected malicious data as invasion, or as a result of the immaturity of the multi-tenant system supported by IoT platforms, whatever the reason this failure will lead to. A dispute will happen between the customer and the provider and so on. So, security remains the obsession for any user and the most important reason not to rely on the cloud and IoT that related it, according to a study released by IDC, it has been found that almost 88.5% of customers stay away from using the cloud for their important data, and their primary reason for refusal that is the security of data, but it should be noted that traditional internal servers are not more secure. For example: in the United States, hackers hacked into the government network, that supposed to be safe and difficult to penetrate, it should be remembered that more than 70% of attacks come from within the organization while emphasizing that providing security in the cloud is more difficult than the traditional system because of its being has different layers and levels.

2 Basic Concepts

2.1 IoT Architecture

Before focusing on the cloud and its security issues in this chapter, we must know the architecture of the Internet of Things that described in four components, as shown in Fig. 1.

- Things: They are classified as uniquely recognizable nodes, primarily sensors or actuators that communicate without human intervention using various methods of connectivity.
- Gateway: serve as mid-layer between things and the cloud to provide security, manageability, and the needed connectivity.
- Network infrastructure: This involves routers, aggregators, gateways, repeaters and other equipment that monitor and secure data transfer.
- Cloud infrastructure: comprises vast pools of virtualized servers and storage that are networked together with computational and analytical capability.

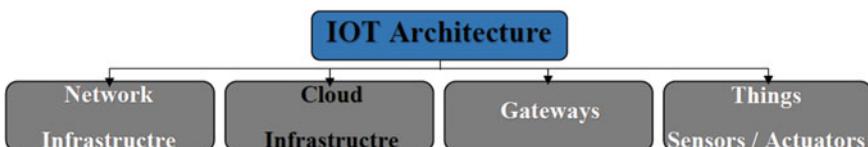


Fig. 1 IoT architecture [1]

2.2 Cloud Computing Architecture

It is known that the cloud consists of three layers, which are SaaS, PaaS, and IaaS, so each provider has its own infrastructure, platform, and software layer [2, 3], as shown in Fig. 2. Thus, when the customer deals with the applications provided by the cloud service provider, he is forced to use the infrastructure and platform that that provider provides. Any breach or attack in IaaS will necessarily affect the security of the other two layers and vice versa, therefore, the cloud service provider has full access to customer data and knowledge of their location [4], which determines the level of abstraction of each layer and the extent of user control, so IaaS has greater control over the client, and control is decreasing towards the upper layers, which increases the security risks in them and vice versa. Of course, each cloud service model has its own security weaknesses in addition to the presence of common obstacles that have an impact on all of them [5], and this increases the security dependency among them [6].

There are different types of attacks and threats that differ depending on the level or the party. Various organizations such as the Cloud Security Alliance are working on identifying security problems that need to be addressed [7].

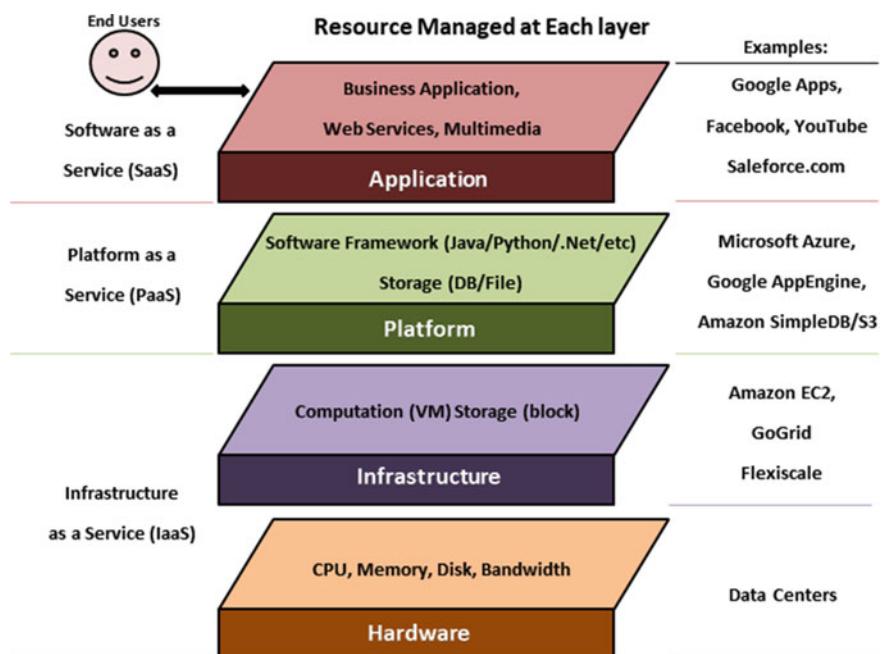


Fig. 2 Architecture of cloud computing [5]

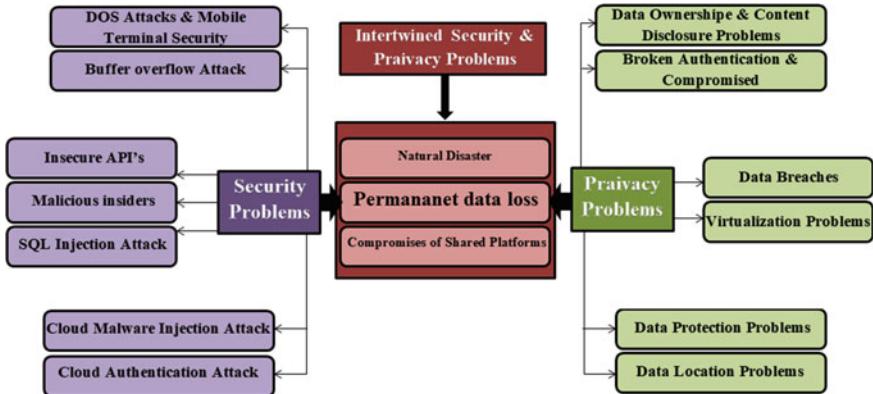


Fig. 3 Security, privacy, and intertwined problems in cloud computing [9]

2.3 *Definition of Security and Privacy*

Security and privacy can be defined according to the following [8]: “Security isn’t to tamper with a user’s items that adversely influence his activities, Privacy is to leave a user’s details to himself only”. It can be said that privacy is the process of hiding an individual’s information and isolating it from others in a dynamic, and selective manner. As for security, it is keeping the information safe and resisting any potential danger or unwanted forced change from others.

Figure 3 shows us security and privacy problems, which focus mostly on information security and loss, and this is what has been worked on in our research through the use of cryptographic algorithms to maintain information security, in addition to using decentralized blockchain technology to distribute data to more than one server in the event of any attack or sabotage.

2.4 *Definition of Cloud Security*

Cloud Security is the data storage/availability of services for users across the cloud platforms via the Internet in a secure and protected against penetration (whether this penetration is for the purpose of deletion or leakage or other), the security of the cloud is a form of cyber-security and consists of a set of controls and technologies that share together to protect the infrastructure and cloud data, Through Fig. 4, it has been represented the problems and classifications of cloud security, which makes it easy to understand attacks, evaluate them, and suggest solutions to them. It also observed from Fig. 4. that to achieve security requires the provision of several things: (such as firewalls, encryption, obfuscation, VPNs, etc.), in addition to that the most important factor in data protection insurance is the nature of the relationship

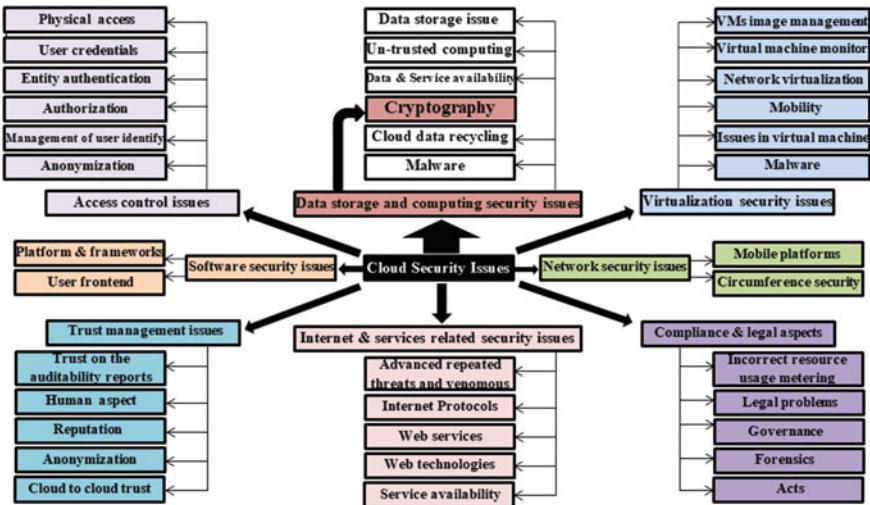


Fig. 4 A review of the security issues of cloud computing [10]

between the cloud service provider and the customer, this is known as the service level agreement SLA, and this is the most important clause between the two parties.

2.5 Cloud Security Items “CIA” and Requirements

As we said cloud security includes maintaining confidentiality, integrity, and availability of data stored in the cloud [11] and to achieve the concept of CIA “ISECT 2014a, CSA 2013b, ISO/IEC 2016”, we need to meet certain requirements such as assurance, trust, governance, monitoring, and strong security, etc. Anyway, the definition of CIA term is given as below.

2.5.1 Confidentiality

Confidentiality is the protection of customer data and the ability to hide it against unauthorized parties, whether these clients are individuals, institutions or otherwise, and confidentiality here does not apply only to customer data but to their services including their applications and others [12], and achieving confidentiality happen by using traditional encryption algorithms [13], taking into account that there is a difference from the traditional storage method, in the cloud and without the customer’s knowledge, his data are distributed across different geographical locations according to the locations of the cloud provider servers “ex: AWS”, in addition, CSP can change the location of the data from one provider to another “VM Relay, especially Direct

Relay [14]” due to several reasons (such as load balancing, maintenance, etc.), so that, confidentiality must be preserved during data transmission, and this change in location will lead to a change in the set of laws applied in the country of origin as a result of data get outside of the original country for customer [15], and this is definitely a threat to the confidentiality of the data within the CSP servers that more than one client can access at the same time [16]. Thus the sensitive data inside it are vulnerable to hackers or curious users, and this access happens via the Internet. So, it should be considered using encrypted channels such as TLS, VPNs, etc. [17].

2.5.2 Integrity

Integrity is to keep the data stored in the CPS completely, to maintain its integrity against any unauthorized modification or access, and to ensure that it can be displayed accurately and consistently so that it does not differ from the original data stored from the beginning. Violations of integrity can lead to unimaginable wrong results (such as violating published information about the COVID-19 virus, tampering with the integrity of the data of those infected with it, and the resulting global catastrophe nowadays) [18]. As we know that the volume of data grows and increases while the storage capacity of the disks is constant, and this leads to an increase in the number of drives by the cloud provider, who will transfer the rest of the data to other disks, and, therefore, there is a possibility of failure and damage of disks or even data loss, so the increase of disks increases the proportion of disability and problems, but it does not increase the speed of obtaining information [19]. Therefore, the user must obtain guarantee from the cloud provider that it is monitoring the integrity and integrity of the information inside the cloud. Integrity is achieved through the use of the Hashing “signature”.

2.5.3 Availability

Availability is the user’s ability to successfully and easily access his information and resources upon request and use it, so that the service provider’s servers are ready and available when necessary and not closed, without regard to cases of hardware failure, power outages, and denial of service attacks [20], because any interruption will mean significant financial losses and many risks. The cloud provider determines availability and its ability to respond to the request based on the service level agreement SLA [11]. There are two strategies that the cloud provider uses to secure and improve availability:

1. Redundancy so that the cloud provider duplicates data on more than one server and in different geographic locations.
2. Hardening is used by Amazon to have the ability to block and filter traffic according to port and IP address.

The CIA concept has been expanded to include the following:

- Non-repudiation: is the entity's ability to assume responsibility for its actions on its data set and not to refuse its procedures, so that the service level agreement between the two parties is confirmed without any denial, and its consequences if it does not apply, significant material losses, in addition to the loss of confidence and reputation [21].
- Authenticity: This means that the information in the cloud provider is original data so that the owner and origin of the data can be ascertained, and this is accomplished by numerous signature schemes [4].
- Reliability: is the ability to deliver results consistently.

There are some other requirements for achieving security, such as: physical security, data sanitization, non-collusion resistance, data segmentation, data traceability and labeling, data location restrictions, backup procedures, authentication. Table 1 gives us the outline of cloud computing security issues.

2.6 *Security in the SPI Model*

As we mentioned, the cloud consists of three layers, which are SaaS, PaaS, and IaaS, so each provider has its own infrastructure, platform, and software layer [23]. Thus, when the customer deals with the applications provided by the cloud service provider, he is forced to use the infrastructure and platform that that provider provides. Any breach or attack in IaaS will necessarily affect the security of the other two layers and vice versa, therefore, the cloud service provider has full access to customer data and knowledge of their location [24], which determines the level of abstraction of each layer and the extent of user control, so IaaS has greater control over the client, and control is decreasing towards the upper layers, which increases the security risks in them and vice versa.

Of course, each cloud service model has its own security weaknesses in addition to the presence of common obstacles that have an impact on all of them [25], and this increases the security dependency among them [6], we will talk about that below.

2.6.1 Software-as-a-Service (SaaS) Security Issues

As mentioned, SaaS provides application services such as email, conference programs, and other applications [26]. The users of this layer have less control over security than other layers, so the security concerns about this layer are rather large. The geographical location of the customer information site is a concern, in addition to that the information is processed and stored in this layer as normal text and therefore must be encrypted to maintain its confidentiality [26], backup storage concerns [27], in addition to that some cloud providers provide users with the ability to jointly access data storage locations (Multiple Leasing Service), therefore CSP must separate any user's data from other unauthorized users. Sometimes a CSP causes a violation of

Table 1 Overview of cloud computing security issues [22]

Issues of security	Attacks	Affected service delivery models	Responsible characteristics of cloud	Threat to C-I-A-A-P	Directions of protection
Virtualization-related issues	<ul style="list-style-type: none"> - Cross-VM attack - Data violations - Application security infringement - Access control infringement 	IaaS, PaaS, SaaS	Multi-tenancy	Confidentiality, integrity, availability	<ul style="list-style-type: none"> - Isolation of VM - Use of trusted VM image - Use of firewall/IDS - Strong authentication - Encryption
Physical security issues	<ul style="list-style-type: none"> - Physical damage to infrastructure - Theft 	IaaS	Broad network access	Accountability, privacy	<ul style="list-style-type: none"> - Backup of data - Backup of application - Reserved resources
Network-related issues	<ul style="list-style-type: none"> - Data violations - DNS server attack - IP-based attacks - Attack on DHCP server - Traffic flow analysis 	IaaS, SaaS	Broad network access	Confidentiality, availability, privacy	<ul style="list-style-type: none"> - Use of firewall/IDS - Encryption
Data-related issues	<ul style="list-style-type: none"> - Modification of data - Deletion of data - Loss of data - Unauthorized access 	IaaS, PaaS, SaaS	Multi-tenancy, broad network access	Confidentiality, integrity, privacy	<ul style="list-style-type: none"> - Strong authentication - Encryption of data - Isolation of data - Backup of data - Use of database intrusion detection

(continued)

Table 1 (continued)

Issues of security	Attacks	Affected service delivery models	Responsible characteristics of cloud	Threat to C-I-A-A-P	Directions of protection
Application-related issues	<ul style="list-style-type: none"> - Application modification - Application interruption - Cross-VM attack - DoS attack - Privacy violations - Hijacking of Session - Impersonation - Cross-site scripting (XSS) attack - Injection of SQL attack 	PaaS, SaaS	Multi-tenancy, broad network access, pay-as-you-use pricing model	Confidentiality, integrity, availability, privacy	<ul style="list-style-type: none"> - Access control - Strong authentication - Use of bug-free applications - Use of firewall/IDS - Isolation of application

customer confidentiality as a result of not completely deleting their data when they request the cancellation of a particular service, and the deletion of part of the data by the service provider may mistakenly be another violation in the integrity of the data, and here the user will not be able to discover this fact, and this is what prompted us in our research to use blockchain technology. Since access to services runs through browsers [22], all web-based attacks must be known as weaknesses in SaaS, Cloud Security Alliance [25] has announced the release of a document describing the reality of mobile computing and the most important challenges in this area, also it must be taken with what the Open Web Application Security Project (OWASP) has identified around the top ten security threats to web applications, such as SQL injection attacks which is able to change user databases, malware attacks, metadata spoofing attacks that is capable of changing what WSDL files contain and cause to unencrypted communication between web services, warp attack while translating SOAP messages in TLS layer (transport layer service), XML signature attack that holds the network protocols (so the XML must be encoded in the main browser side), and other types of attacks through which the hacker interrupts activation the performance of the usual cloud servers [28] and affects in data integrity. The denial-of-service attack in the cloud system is the most important reason for the lack of service or data so that a large number of random requests are sent to dump the service, and here the role of CSP lies with providing more services.

2.6.2 Platform-as-a-Service (PaaS) Security Issues

This layer publishes the applications developed by the customer without any need to purchase software and maintenance costs [27], also here we need a network and a secure browser. The security in PaaS applications consists of two parts: the security of the PaaS layer itself and the security of the client applications in this platform PaaS [9], which requires the CSP to provide the basic system software package in order to ensure that applications operate safely, and since PaaS provides components of web in addition to the traditional programming languages, so it suffers from the same problems that the web suffers like data and network security, and we must take precautions when dealing with third-party services (the third party), and as a result of the rapid growth of the cloud, developers must constantly update their applications in PaaS with consideration Development Life Cycle (SDLC) and the related security aspects, in addition to that, developers should have knowledge about the legal aspects of data storage sites so that they do not expose themselves to security holes, PaaS suffers from the problem of multiple tenants, finally and even in the event that the developers were able to control over the security of their applications, they cannot provide any guarantees that the basic infrastructure they use is safe, and this is the responsibility of the provider.

2.6.3 Infrastructure-as-a-Service (IaaS) Security Issues

We know that IaaS offers a different set of resources, such as servers, storage media, networks, and other computing structures, in the form of virtual machines accessed by the Internet, and these devices operate, control, and manage resources [29]. IaaS enables cloud users to better control security compared to other models, as there is no security vulnerability in the virtual machine screen [27], with the need to take into account some threats such as: Registering a client in the cloud as root and obtaining his permission to access more virtual devices and this what makes user data threatened (impersonation), also the problem of multiple burden work as a result of sharing work on the same virtual servers so that the workload must be isolated which is very important so that the resources are divided among all the workloads in the data centers, using VMM (Virtual Machine Manager or Hypervisor) is a low-level program that controls and monitors its virtual machines, which is like any traditional program that faces security flaws but reduces threats because it facilitates the process of finding and fixing errors. Virtual Machine Image (VMI) are created by either the provider or the customer and is also vulnerable to malware. Another threat associated with Virtual Machine images is that VMIs may store customer or previous owner information, and this is what is feared to be used by another user, so VMIs must be deleted well by CSP before using it from another client, virtual networks or VLANs must also be isolated to get away from the unauthorized flow of data through them, one attack is the other is when one of the hackers runs its own malicious service instance or virtual machine instance, and, thus, the opponent is tricked into using the instance as Valid. Also, VM repetition is one of the reasons that lead to data leakage so the user must pause the devices during replication to ensure that the data are integrated [30], the ability of VM devices to move between different data centers according to the CSP request is one of the important characteristics of it (its displacement for load balancing [30]), but this makes its security at risk, for both VM escape and VM hopping significant risks to security and data confidentiality as well, there are some concerns regarding service availability or failure of a VM using another alternative instance [27], as a result of DoS attacks On servers.

Therefore, you should always pay attention to the safety of virtual machines and the life cycle of VMs as well as VMIs, yet the primary controller remains the Cloud Service Provider. Table 2 gives us the outline of cloud service delivery models according to security issues.

2.7 *Cloud Storage*

It is considered a sophisticated model capable of converting storage and computing capabilities into the hands of external service providers (CSP), but as a result of the loss of direct control of data, users are reluctant to use cloud services, as data security and privacy is one of the most important challenges that concern users, for example in 2013 the Washington Post announced that The US National Security

Table 2 Cloud service delivery models according to security issues [22]

Service delivery model	Elements of key security	Threats of possible
Software-as-a-service (SaaS)	<ul style="list-style-type: none"> • Security of web application • Control of access • Security of software • Services availability • Confidentiality of data • Integrity of data • Privacy of data • Backup of data and application • Authorization and authentication 	<ul style="list-style-type: none"> • Data violations • Breaches of privacy • Hijacking of session • Impersonation • Cross-site scripting (XSS) • Violation of access control • Attacks of SQL injection • Deletion of data • Analysis of traffic flow • Attacks of cross-VM • Attacks of DoS
Platform-as-a-service (PaaS)	<ul style="list-style-type: none"> • Control of access • Security of application • Application data security • Availability 	<ul style="list-style-type: none"> • Impersonation • Data violations • Modification of application • Interruption of application • Attacks of cross-VM • Attacks of DoS
Infrastructure-as-a-service (IaaS)	<ul style="list-style-type: none"> • Physical security • Availability of services • Data confidentiality in the storage • Data integrity in storage • Protection of virtual cloud • Security of network • Data violations during transmission through a network 	<ul style="list-style-type: none"> • Physical damage to infrastructure • Attacks of DoS • Attacks of DNS server • Attacks of IP-based • Attack on DHCP server • Analysis of traffic flow

Agency (NSA) is spying between Google and Yahoo data centers around the world, and therefore more than 54% of German companies are finding that using the cloud is a concern according to a poll published in 2013 by Price Waterhouse Coopers (PWC). Therefore, a reliable cloud provider must be used in addition to maintaining data confidentiality through encryption and maintaining its availability as well [31].

We concluded that most of the security problems related to data are concentrated in the SaaS and IaaS layers where our work will be concentrated in this research, noting that most of these threats can be solved by segmenting and encrypting information to maintain its confidentiality, and this is what will lead us to talk about cryptography and hashing, also by data authentication and the use of hashing algorithms to maintain data integrity, finally distributing data to more than one server to maintain their availability, and this is what the blockchain technology will provide.

2.8 Cryptography

As a result of the importance of maintaining the confidentiality of the data stored in the infrastructure of the cloud, we have to talk about the symmetric and asymmetric cryptographic algorithms as shown in Fig. 5, with the need to an important mention that the symmetric algorithms are the most important in cloud applications and services that need encryption due to the greater security force they possess [32]. Cryptography: is a mix between mathematics and computer science, in which data are obfuscated and hidden during transfer to be confidential between the two parties (sender/receiver) and cannot be read by unauthorized people who do not have key decryption. Cryptography takes into account basic requirements that are confidentiality, integrity, availability, key management, and non-repudiation.

When we talk about cryptography, it should be mentioned that asymmetric key algorithms are not efficient enough for small portable devices because they require more calculations and memory [34], however, there are many protocols that work according to asymmetric algorithms like SSH, PGP, S/MIME, and SSL/TLS, GPG, ZRTP, Internet Key Exchange, and SILC. In contrast, symmetric key algorithms are about 1,000 times faster because they require less math processing capacity. This is why in our research we chose data encryption using a symmetric key algorithm because the speed of encoding the data flowing in the cloud is very important. We chose AES because it is the standard and common algorithm for data encryption (NIST). It is true that symmetric algorithms are fast in the encryption process, but their problems are concentrated in: fear of brute force attacks that rely on the use of symmetric encryption cracking tools so that they depend on the characteristics of the algorithm to discover the secret key and thus the hack occurred [32]. Therefore, asymmetric algorithms were used to encrypt the symmetric key algorithm, and as we know symmetric algorithms are slow but safe because they rely on large mathematical operations that make their penetration almost impossible and the most common asymmetric algorithms are: RSA and ECC. But looking at the researches, it turns out that the ECC algorithm outperforms RSA with operational efficiency, security, and with fewer parameters and the same key length as 256 recommended by NIST. ECC is the fastest, most secure, and the lowest memory consumption, so ECC is the most convenient [35].

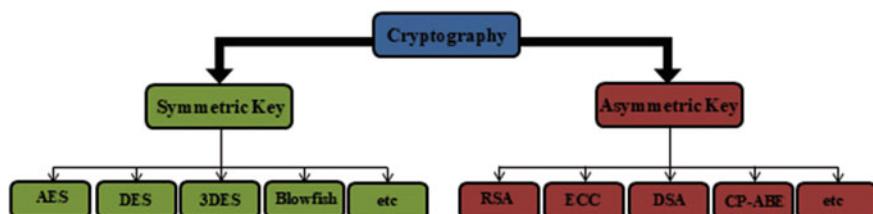


Fig. 5 Classification of cryptography algorithms [33]

Fig. 6 Hash algorithm diagram



2.9 Hashing

Hashing is one of the concepts of unidirectional encryption since the plain text cannot be retrieved from the ciphertext as shown in Fig. 6, as the data are compressed to a standard fixed size regardless of its original length, and no keys in hashing are used for encryption or decryption. The ciphertext is generated from the plain text [32].

The hash algorithms are used to maintain the integrity of the data, as the digital signature algorithm DSA uses a secure hash algorithm (SHA) to create signatures and verify them. DSA is one of the asymmetric algorithms, where the sender uses the private key to create the digital signature, while the receiver uses the public key for signature verification, DSA has been developed by NIST, and its functions are summarized in signature and verification [33]. Hash keys are also generated by the SHA algorithm, and this hash is required to retrieve files. The Hash algorithms have several types, the most famous of which are: MD5, SHA, but the SHA family remains the most famous as we note through its applications and because of its security, as SHA's algorithm is an encryption hashing algorithm designed by the national security agency (NSA) and announced by the National Institute of Standards and Technology (NIST). This algorithm can compress the given information and give a hash key 160-bit (20-byte). Of course, to choose one of the hash algorithms (MD5, SHA-1, SHA-256, and SHA-512), several factors the most important of which are safety, speed, and nature of use, must be taken into account. From the security aspect, MD5 and SHA-1 were excluded as a result of their penetration. SHA-256 and SHA-512 belong to the most secure SHA-2 family [36], where SHA-256 is calculated in word 32-bit, and SHA-512 with word 64-bit, it should be noted that SHA-256 is much faster than SHA-512. So, I chose to rely on SHA-256 because it is the fastest and because the nature of use within the blockchain technique requires that [37] as all research papers use SHA-256 with blockchain technology.

2.9.1 Blockchain Technology

Maintaining data integrity and availability is done through blockchain technology, which appeared for the first time in the form of digital currency (Bitcoin) for digital games and was designed by Nakamoto in 2008, then began to increase in popularity. Blockchain is a decentralized P2P network so that the user and his counterpart are able to manage it without a central authority away from the fees imposed by the third party [38], as shown in Fig. 7.

Blockchain is a decentralized distributed technology that employs a variety of encryption patterns, it represents a database of all digital transactions and events that take place between participants. Blockchain technology consists of an organized series of blocks containing information records, each block representing a structure

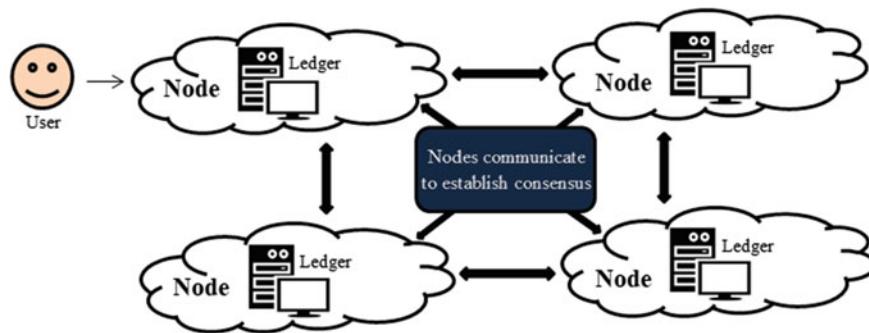


Fig. 7 Blockchain technology in P2P architecture [37]

consisting of a head that contains hash and timestamp and an index (previous hash) to link the block to the hashing of the block that precedes it directly in the form of a stack, and the body represents the data, as shown in Fig. 8.

The first block represents the formation mass and indicates the entire blockchain when any new block is created placed over the previous layer as a heap. The system is responsible for monitoring the chain and updating it repeatedly when any new block [52] arrives at each point of failure (the authorized third party) [51], the search of the block information in the database is done by index way [39]. Hashing is resistance to decryption and is created via the secure algorithm (SHA-256), which ensures the hardness of the chain of information created, because any modification of the blocks will be immediately detected via hashing because the value of each hash is affected by the values of the previous blocks, in addition to improving security through a placed copy of each block in among all the nodes participating in the cloud (the nodes are the same as a ledger and represent the server) [37]. The adoption of blockchain helps to make storage safe (able to withstand Byzantine failure), decentralized, easy to monitor, available, transparent, coherent, and resistant to tampering attempts, as the process of detecting any modification is easy because it is not possible to replace or delete any stored record except after the compatibility of the majority of the participating networks and the consent of the stakeholder (it is a consensus algorithm), however, data can be changed and penetrated if 51% of the peers are forged simultaneously and this scenario remains difficult to achieve [39]. Each share node maintains

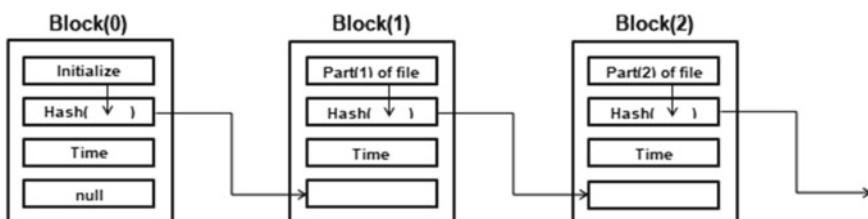


Fig. 8 General diagram of Blockchain

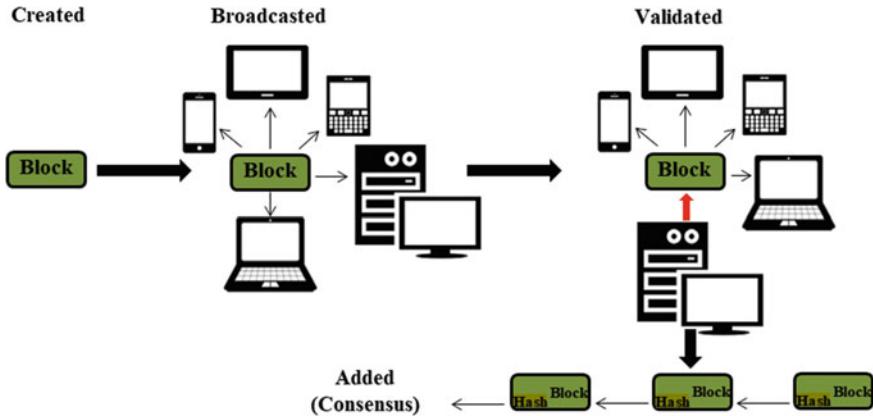


Fig. 9 A typical Blockchain work flow [41]

its own copy of the ledger, as it is compared with the central registry server to ensure authenticity and integrity [40], and each node updates its version when any new transaction is received [39]. Finally, we confirm that data piracy has become difficult due to its presence in more than one node using the blockchain, in addition, that the blockchain achieves the standards of speed and low costs, implementation, and easy use in addition to its ability to expand, and thus the future will be for it [39], as shown in Fig. 9.

Therefore, we used the cryptography as a traditional solution to keeping data confidential by encrypting it in the SaaS layer using the AES algorithm, whose key is encrypted with the ECC algorithm to ensure a better level of security against any breach, and that ensure better performance because AES and ECC are the best among the symmetric and asymmetric algorithms. To maintain the integrity of the data against any tampering, hashed using the SHA-256 algorithm, which is the best among hashing algorithms, and this hashing is embedded within the decentralized distributed blockchain technology that ensures the availability of data as well. Thus, the required security elements of CIA for data stored in infrastructure in the cloud have been achieved against any type of possible breaches and threats.

3 Related Work

First, we have to talk about some of the reviews that talked about the use of blockchain technology, mentioning that all of them are recent: In this study [42], a new mechanism was proposed to maintain data security against unauthorized access either during the transmission process through the Internet or while it is at the cloud service provider, where the data are encrypted by a blowfish symmetric algorithm and its secret key is encrypted by the asymmetric RSA algorithm, and this is a stage hybrid

encryption to obtain data confidentiality, the next stage was done using the SHA-2 and DSA algorithm to achieve digital signature and thus maintain the integrity of the information. This study [43] suppose an idea of avoiding weaknesses in dealing with public key certificates, and the proposed security against counterfeiting and hacker attacks through symmetric linear signature based on identifiers according to Oracle's random pattern via blockchain technology. This talking [44] about using a blockchain to ensure data integrity and protection it against counterfeiting and misuse by performing authentication and review transactions, which is a lightweight alternative to the MAC algorithm that requires the presence of two entries: secret key and variable-length data, so this algorithm (MAC) computes value in user side for authentication, and the data is stored in external resources in the cloud, whenever the information owner needs to ensure its integrity, which has to be redownloaded it and contrasted with the MAC value, therefore, there will be a large calculation cost. Another suggestion is to solve the problem of ad-hoc data access safely, using the blockchain technology to control the information stored in the cloud away from the presence or intervention of a third party and without the problems of redundancy experienced by participants in cloud storage services [45]. Managing sensitive and huge data for smart homes and other critical systems resulting from the Internet of Things and protecting them and ensuring that no cases of forgery have occurred by applying blockchain technology instead of sending that information to one central server with the security challenges it carries [46]. Introduce the idea of an improved customer identity management system by applying blockchain technology enables network access via a pseudonym out of the access identity and rebuilding subscriber IDs [47]. Checking the sources of data in the cloud and discovering cases of fraud through the ProvChain structure consists of three steps: collecting source data and then verifying and maintaining its privacy against change by using blockchain [48]. The use of a blockchain decentralization structure is to check data integrity and availability [49]. A hybrid algorithm is proposed using a combination of Blowfish, AES, and ECDH so that build authentication and data security layer before you save it in the cloud [50]. The use of a blockchain will provide a decentralized infrastructure that ensures the concept of identity authentication and prevents DDoS attacks that affect the cloud's infrastructure and data stored in it, which positively reflects on security issues [51]. A distributed model proposal provides a secure connection away from problems associated with the insecure data collection process in the cloud, using IPFS (Inter Planetary File System) and blockchain (Cryptouch) [52]. Blockchain technology can be applied to electronic health records (EHRs) so that patients are able to control and manage their medical records without hospital intervention, where multiple powers are used with a pair of keys so that each patient has a public and private key to resist any attempt of counterfeiting in addition to providing a security signature MA-ABS schema to repel hacker attacks [53]. In this study [54], it was talked about the application of health care systems for blockchain technology in order to protect patient data and maintain its availability upon request and put it in a distributed manner between health centers in a safe and integrated way, and it is expected to increase the spread of the use of the cloud and data protection techniques in it such as blockchain especially after the spread of COVID-19.

4 Methodology

To maintain the data security of cloud user, we include two new layers in the cloud, where the first layer (encryption/decryption) is integrated into the SaaS layer, which guarantees the user the confidentiality of his information while moving over the Internet or against hackers and intruders from the cloud service provider (CSP) employees, and this hybrid layer consists of AES and ECC algorithms, where the AES secret key is a user password or is randomly generator, that is encrypted through an asymmetric ECC algorithm whose public key is randomly generated (by RNB random number generator), in order to prevent that of AES secret key from being forced attacked and as a key distribution mechanism by ECC, so that each user has unique keys from other users and without the intervention of the cloud service provider, which leads to increased security for each user, and after creating the keys, the data are encrypted using AES, and the length of the key is 128 bits, which is the same length of the encrypted data block. As for the second layer, it represents the blockchain and is integrated into the IaaS layer, which guarantees the user the availability and safety of its information via the hash algorithm (SHA-256) found within the blockchain, where the encrypted data are divided into digital signature(hashing), then it is stored in the blocks of the chain to ensure the integrity of the data by comparing the data hash values encrypted within the chain blocks, as shown in Fig. 10.

The work will be divided into two levels:

1. The front user interface:

It represents the SaaS layer and is either a web application or an Android application as it is in our research, and this application provides the ability to deal with data stored in the cloud (upload/download). When the customer chooses a file to store in the cloud, the ECC public key is randomly generated and encrypts the secret key of the AES algorithm, AES will encrypt the file that has been divided into blocks of length 128 bits the same length secret key of the AES algorithm, after which the segmented encrypted data are pushed into the infrastructure of the cloud. Fragmentation is useful for speeding up transferring the files to the cloud. In the case that the user wants to download the file, the same process is performed but in reverse, where the secret key of AES is decrypted using the ECC private key, then the data blocks are decrypted using AES and checked for integrity and collected to obtain the original file.

2. The back end:

It is represented by IaaS as the cloud service provider infrastructure layer, and in our research, we used a local server to store data instead of service provider servers like AWS and others. After the encrypted data are pushed to store, the encrypted data are divided into a fixed length, and the digital signature is created. Therefore, for every chain that belongs to a specific user, the hashing signature of the encrypted data is stored in the blockchain according to timestamp with the storage of other parameters (hash and previous hash). We wrote our code inside the virtual cloud so that the

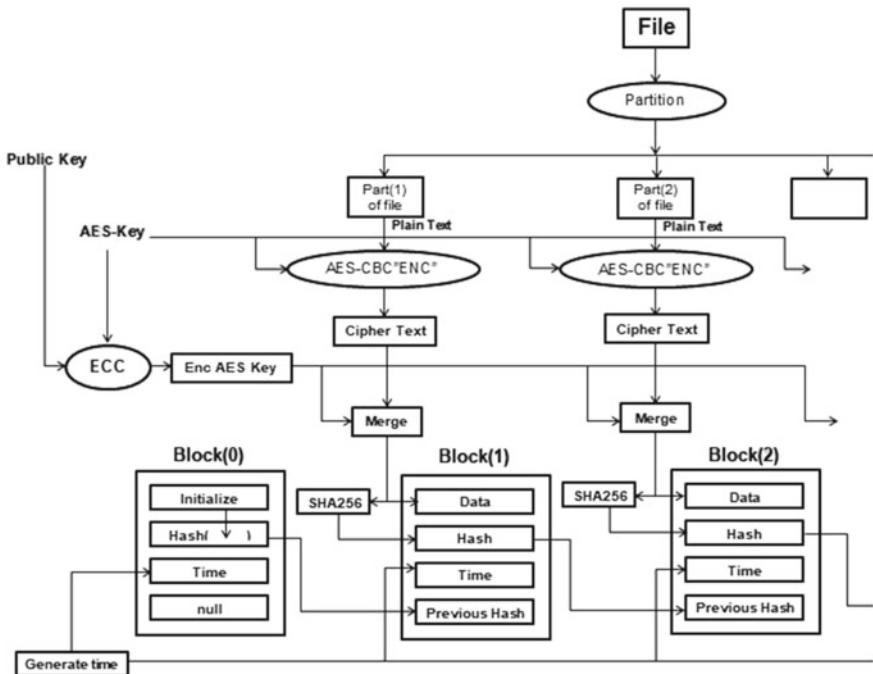


Fig. 10 The Encryption process with creating a Blockchain and using ECC and AES

data are verified to match its digital signature (hashing) periodically to ensure its integrity, and to ensure the chain block is consistent with each other, the hash value of each block is compared to the hash value of its previous block. In addition, that when downloading the data, for confirming the integrity and availability of data in the distributed network via blockchain, the chain of blocks that the user wants to download is compared with the same chain of blocks, but in another node (ledger) to verify its integrity and not forge to tampering. The work is done in a sequence and coordination between the front and back end starting from uploading data to the cloud, creating and distributing keys, encryption, hashing, verification, and even creating chain blocks. The download process is done in reverse.

5 Result and Decision

The work is implemented through several stages, as we initially considered that the hybrid encryption layer consists of AES, RSA, and PBKDF 2 algorithms, but the results are shown of the negative use of PBKDF 2 in consumes of time without achieving significant security benefit, then after that, we decided to use only AES and RSA algorithms, but after reading more researches, we found that the ECC algorithm

is better than the RSA algorithm, and thus our work became based on the use of AES and ECC algorithms in the hybrid encryption layer, we show you the steps of work and results.

First, AES, the algorithm was chosen to encrypt the data, which is the best and most used symmetric algorithm according to the scientific references as we mentioned previously. In addition, the key of the AES algorithm was encrypted via the RSA algorithm, which was found firstly among its peers in asymmetric algorithms according to NIST. The PBKDF2 (Password-Based Key Derivation Function 2) are key derivation functions, used to reduce vulnerabilities of brute force attacks and for password hashing, which are considered the best among their counterparts' password hashing schemes, as shown in Fig. 11.

Thus, the data have become encrypted in the SaaS layer in the cloud as confidentially, and to maintain its integrity also has generated Hash for encrypted-data to make the blockchain in the IaaS layer in the cloud. The best one is SHA 256 It is much faster and secure than other hash functions. We also know that creating a hash for the data makes it impossible to attack the data itself because if the data are attacked, the corresponding hash will reset it when it is restored again. But the fear here comes from the possibility of attacking the Hash itself, hence the need to use the blockchain. Finally, the application of the decentralized blockchain technology, which will generate a series of interconnected hashes that will be difficult to break, remains because, in the event of attacking any hash and trying to replace it, the attack will be discovered immediately, regardless of the type or place of attack. Figures 12 and 13 show the decryption and encryption process.

The encrypted data that make up the Blockchain are stored in the cloud as shown in Fig. 14, also the role of blockchain technology comes from its role in detecting attackers.

The blockchain technology is used to detect the attack among nodes and return data to its original state. The data can return to normal by matching and consensus with the other nodes. Figures 15 and 16 show the node with valid data and attacked node.

The time of implementation of the PBKDF2 algorithm, bearing in mind that the length of the salt is 256, the Iteration Count (IC) is 6 and 8, and the password is made

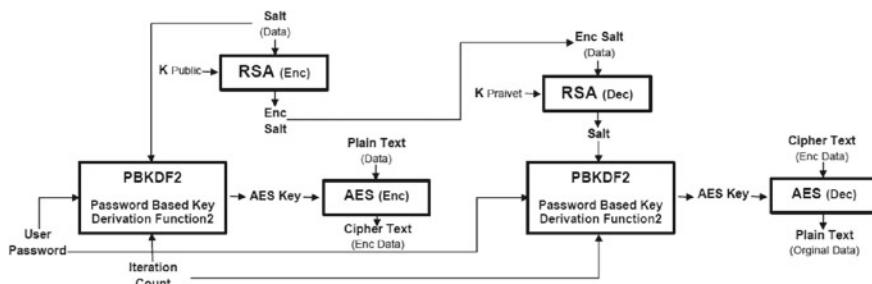


Fig. 11 Encryption/Decryption process using RSA and PBKDF2 on AES key

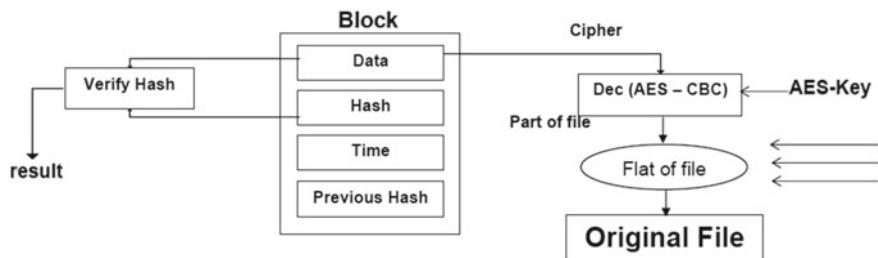


Fig. 12 The Decryption process and create a verify

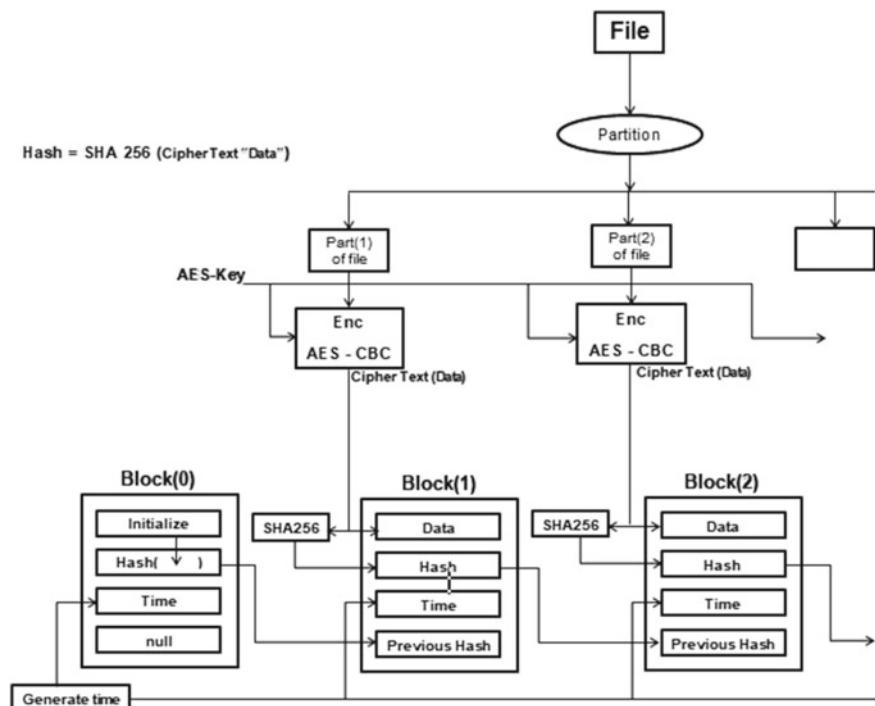


Fig. 13 The Encryption process with creating a Blockchain and using RSA and AES

up of only eight characters “uppercase and lowercase letters and numbers only”, where were used 100 passwords, is shown in Figs. 17 and 18.

The implementation time range is between 0.4 s and 0.8 s depending on the experiment, while this time would be much greater if the iteration count was more, in addition to another effect which is Increasing the length of the password and forming it from all keyboard characters, all of this will lead to a significant increase in performance time and the capacity of memory. As we know that one of the most important uses of PBKDF2 is to resist brute force attacks that can occur when the keys

General Diagram Of BlockChain

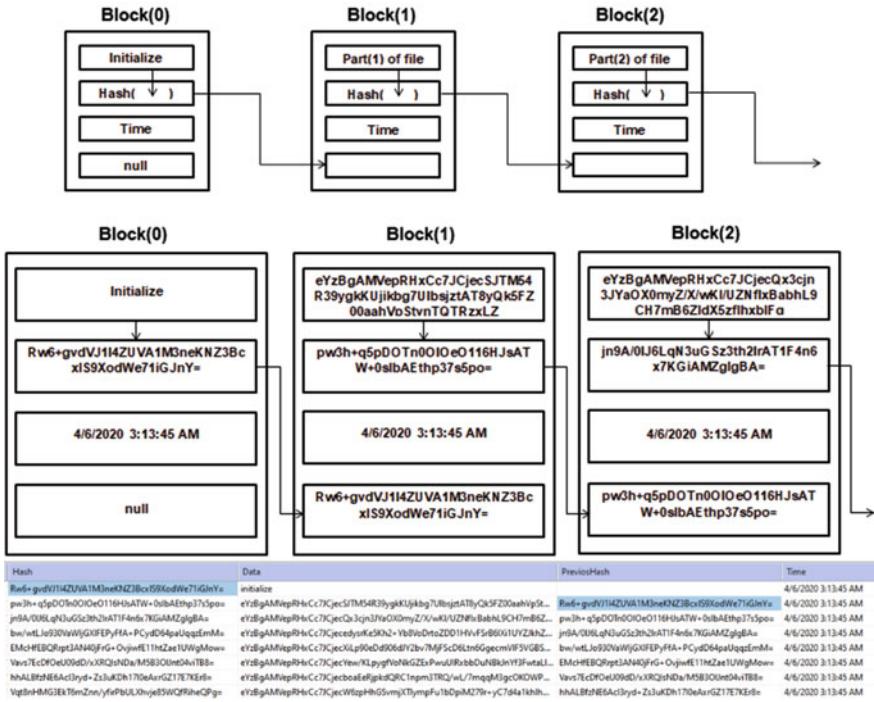


Fig. 14 The diagram of Blockchain with encrypted data

Hash	Data	PreviousHash	Time
Rw6+gvdVJ1I4ZUVA1M3neKnZ3BcxiS9Xo...	initialize		6/12/2020 4:15:23 PM
vlfJ6+q5p0Tn0OIOe116HJsATW+0slbAEthp37s5po...	cJu4Zl2Kc2kBlbOdmx6jlVg7FFKw...	Rw6+gvdVJ1I4ZUVA1M3neKnZ3BcxiS9Xo...	6/12/2020 4:15:23 PM
/ImwKAsA33ic+6NtKuQhPtStH7THK3epl...	cJu4Zl2Kc2kBlbOdmx6jlQbzA2w...	vlfJ6+q5p0Tn0OIOe116HJsATW+0slbAEthp37s5po...	6/12/2020 4:15:23 PM
9RBbhcWNssdEA1RHE0mwlrQEb4JMu8d...	cJu4Zl2Kc2kBlbOdmx6jlxE4Gd003...	/ImwKAsA33ic+6NtKuQhPtStH7THK3epl...	6/12/2020 4:15:23 PM
w8G3H1eV1gxEHP9WCWRkkqYSw/UmyK...	cJu4Zl2Kc2kBlbOdmx6jeAKzBfc...	9RBbhcWNssdEA1RHE0mwlrQEb4JMu8d...	6/12/2020 4:15:23 PM
w55OnUNEBoeY++Kyd5w1QxrZuyNlw...	cJu4Zl2Kc2kBlbOdmx6jlQRzrm+vs...	w8G3H1eV1gxEHP9WCWRkkqYSw/UmyK...	6/12/2020 4:15:23 PM
15h/qDa/6NEsAj83EvvSeBD501Udth8j3h...	cJu4Zl2Kc2kBlbOdmx6jeSmx9Kf...	w55OnUNEBoeY++Kyd5w1QxrZuyNlw...	6/12/2020 4:15:23 PM
R2r73qs9FEZlidC4D0Ns6lDnhCmXj8Ueo...	cJu4Zl2Kc2kBlbOdmx6jlSqi7G+JRG...	15h/qDa/6NEsAj83EvvSeBD501Udth8j3h...	6/12/2020 4:15:23 PM
eZuoAgRTUfl/nL3ClOHv0mRbRpacyzKjK...	cJu4Zl2Kc2kBlbOdmx6jlVvgUgtf...	R2r73qs9FEZlidC4D0Ns6lDnhCmXj8Ueo...	6/12/2020 4:15:23 PM
8eZqYKMRPcBt3w3oXptE4Opwf3ce34H...	cJu4Zl2Kc2kBlbOdmx6jlW7RKwnf...	eZuoAgRTUfl/nL3ClOHv0mRbRpacyzKjK...	6/12/2020 4:15:23 PM
PZlijma1bcqdq17hvBd9aJ0qUvalpzxXGd...	cJu4Zl2Kc2kBlbOdmx6jlVsRL3QK...	8eZqYKMRPcBt3w3oXptE4Opwf3ce34H...	6/12/2020 4:15:23 PM
ZbnOaO1/6/PlmAkDvnLrEzZ+pUOSDAj...	cJu4Zl2Kc2kBlbOdmx6jlewOIJfjs...	PZlijma1bcqdq17hvBd9aJ0qUvalpzxXGd...	6/12/2020 4:15:23 PM
mHu4A+0lwXyMkGGdxNkL9PrMayMc...	cJu4Zl2Kc2kBlbOdmx6jlSf3ey6TG...	ZbnOaO1/6/PlmAkDvnLrEzZ+pUOSDAj...	6/12/2020 4:15:23 PM
U36R7hD/crLihngEw1JS4bCUkgMhx/QvZ...	cJu4Zl2Kc2kBlbOdmx6jlVm84XB...	mHu4A+0lwXyMkGGdxNkL9PrMayMc...	6/12/2020 4:15:23 PM
yas+WNX8HDTofLxzaa1j3Rp9y7lkHe84Lat...	cJu4Zl2Kc2kBlbOdmx6jlSM62iCeF...	U36R7hD/crLihngEw1JS4bCUkgMhx/QvZ...	6/12/2020 4:15:23 PM
ezHtizPPPlusWQrDopnwnGjsKAxsj0ubls...	cJu4Zl2Kc2kBlbOdmx6jlW0Qqold...	yas+WNX8HDTofLxzaa1j3Rp9y7lkHe84Lat...	6/12/2020 4:15:23 PM

Fig. 15 The node with valid data

Hash	Data	PreviosHash	Time
Rw6+gvdVJ1I4ZUVA1M3neKnZ3BcxIS9Xo...	initialize		6/12/2020 4:15:23 PM
vIVj6Pvu1mUzT/IUx6/WvmuamhCov4oL...	clu4Zl2Kc2kB1bOdmx6jlYg7yFFKw...	Rw6+gvdVJ1I4ZUVA1M3neKnZ3BcxIS9Xo...	6/12/2020 4:15:23 PM
/ImwKA4sA33ic-6NTkuQhpStHi7THK33epi...	clu4Zl2Kc2kB1bOdmx6jlQlslw72t...	/ImwKA4sA33ic-6NTkuQhpStHi7THK33epiAb...	6/12/2020 4:15:23 PM
9RBBlcWNssdEA1RHE0mwlrQEb4JMuBd...	clu4Zl2Kc2kB1bOdmx6jlQlslw72t...	/ImwKA4sA33ic-6NTkuQhpStHi7THK33epiAb...	6/12/2020 4:15:23 PM
w8G3H1eV1xgEHP9WCWRkkqYSw/UmyK...	clu4Zl2Kc2kB1bOdmx6jlQkbfCe...	C.V.RamanGlobalUniversity20209RBBlcWNs...	6/12/2020 4:15:23 PM
w55OnUNEBoeY+Kyd5w1QxrZuynWjw...	clu4Zl2Kc2kB1bOdmx6jlQZRm+vs...	w8G3H1eV1xgEHP9WCWRkkqYSw/UmyKsd...	6/12/2020 4:15:23 PM
15h/qbA/6NEAj83EvwSe0D501Udth8J3h...	clu4Zl2Kc2kB1bOdmx6jlEsmn9Kif...	w55OnUNEBoeY+Kyd5w1QxrZuynWjw7Q...	6/12/2020 4:15:23 PM
R2r73q9FEZlidC4D0Ns6lDnhDcMj8Ueo...	clu4Zl2Kc2kB1bOdmx6jlTg+JRG...	15h/qg/6NEAj83EvwSe0D501Udth8J3h4...	6/12/2020 4:15:23 PM
eZuoAgRTUH/nL3CIQHOvNmRbRpacyzKj...	clu4Zl2Kc2kB1bOdmx6jlWvgUgtf...	R2r73q9FEZlidC4D0Ns6lDnhDcMj8Ueodu...	6/12/2020 4:15:23 PM
8eZqYKMRpcBT3w3oXptE4P0wf3ce34lh...	clu4Zl2Kc2kB1bOdmx6jlWTRKwnf...	eZuoAgRTUH/nL3CIQHOvNmRbRpacyzKj...	6/12/2020 4:15:23 PM
PZlijmA1bckdq17hvBd9aJ0qUavlpzxKG...	clu4Zl2Kc2kB1bOdmx6jlWsRL3QtH...	8eZqYKMRpcBT3w3oXptE4P0wf3ce34Hh9Vi...	6/12/2020 4:15:23 PM
ZbnOa01/6/PimAKdvnLrZzE+pUOSDAj...	clu4Zl2Kc2kB1bOdmx6jlWv...	PZlijmA1bckdq17hvBd9aJ0qUavlpzxKGd...	6/12/2020 4:15:23 PM
mHu4A+0lwvXyMkGGdxNkXL9PmMayMc...	clu4Zl2Kc2kB1bOdmx6jlSrF3ey6TG...	ZbnOa01/6/PimAKdvnLrZzE+pUOSDAjBc...	6/12/2020 4:15:23 PM
U36R7hD/crLihngEw1S4bCUkgMhx/QvZ...	clu4Zl2Kc2kB1bOdmx6jlVm84Xb...	mHu4A+0lwvXyMkGGdxNkXL9PmMayMcAes...	6/12/2020 4:15:23 PM
yas+WNX8HDT0fLxzaa1j3Rp9y7lkHe84LA...	clu4Zl2Kc2kB1bOdmx6jlISM62iCoF...	U36R7hD/crLihngEw1S4bCUkgMhx/QvZH2...	6/12/2020 4:15:23 PM
ezHTicPPLuSWQrDopnownGjsKaxsj0ubIs...	clu4Zl2Kc2kB1bOdmx6jlW0gQold...	yas+WNX8HDT0fLxzaa1j3Rp9y7lkHe84Lat...	6/12/2020 4:15:23 PM

Fig. 16 The node has been attacked and the data have been modified

PBKDF2-IC 6

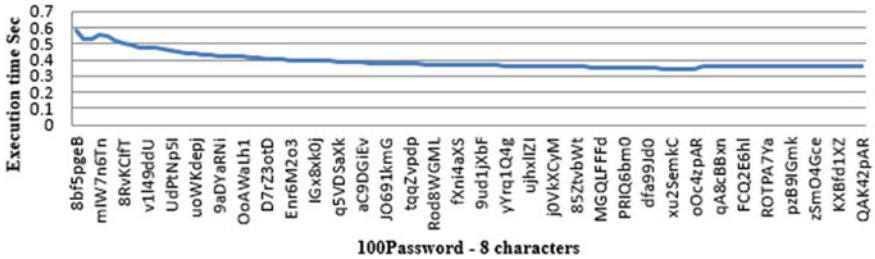


Fig. 17 The Execution time of PBKDF2 in Encryption/Decryption process when IC = 6

PBKDF2-IC 8

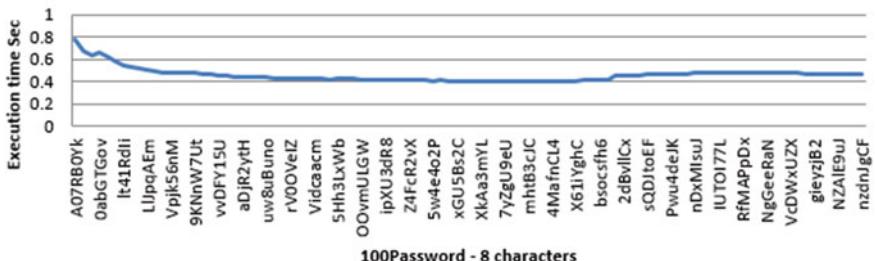


Fig. 18 The Execution time of PBKDF2 in Encryption/Decryption process when IC = 8

of symmetric algorithms move between the encryption process and decryption, but the RSA and ECC algorithms have been able to solve the brute force problem as we mentioned. So as a result of decreased time performance when using PBKDF2, we have decided it to neglect its use, which would lead to an improvement in performance

time with no significant change in security, because the RSA algorithm will be sufficiently safe against brute force attack, especially with the length of the key is 256 bits.

Figure 19 shows the enc/dec process for AES key using RSA, where the RSA decryption is not as effective as the encryption process [35] that the decryption process took much more time than the encryption process time, otherwise ECC has shown better efficiency and security than RSA, so we are using ECC, the ECC is slow in encryption, but it is faster in decryption [35]. We have to remember that the security aspect of ECC is much better than RSA, as the ECC with a key length of 256 bits equals the same level of security in RSA with a key length of 3072 bits. The increase in the key length in RSA to achieve the same level of security in ECC leads to an increase in time, memory and energy consumed, thus becoming Relying on the ECC algorithm with an oval curve is very important because its implementation requires less storage and calculations and hence better, and this is why we rely on ECC as a significant improvement in our research [31]. Table 3 gives us the equivalent security level of RSA and ECC key size.

Security has been improved by generating hash from three factors (Data, Timestamp, and previous hash) instead of only data, with very little difference in performance time, as shown in Fig. 20.

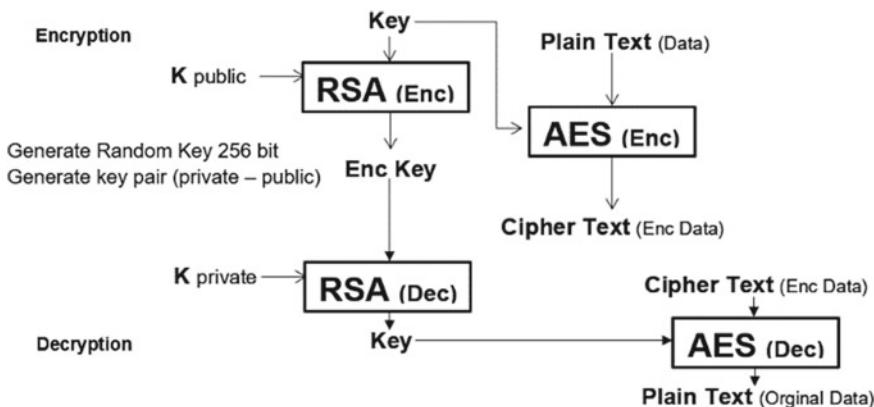


Fig. 19 Encryption/decryption process for AES key using RSA

Table 3 RSA and ECC key size for equivalent security level [31]

Security level Lk, where Lk presents the length of a symmetric key k	80	112	128	192	256
ECC key length (bits)	160	224	256	384	512
RSA key length (bits)	1024	2048	3072	7680	15,360

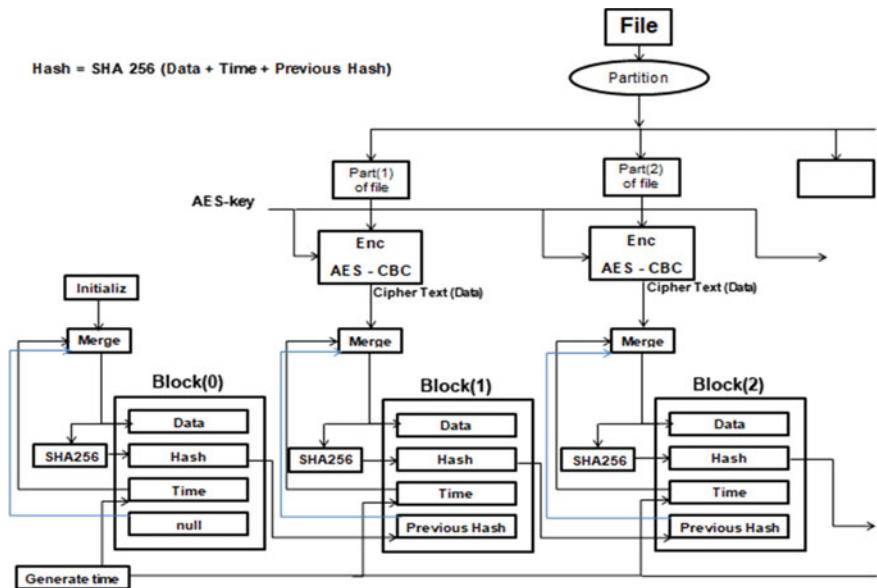


Fig. 20 The process of creating the hash in blockchain using three inputs

Figure 21 shows the time when hashing if it was created from: data only, or (data, previous hash, and the time stamp), where the size of each block in chains will be 100 KB (fixed), and the size of the data will be different up to 25 MB.

We noted that the process of generating a hash from three elements (data + timestamp + previous hash) instead of just generating it from the data will provide greater security, but with a negative impact on the performance of course, and this is what has been noticed by experiences, where the performance time varies between the previous two methods according to the size of the block (the original file size), where the performance is almost the same when the block size in the chain is less

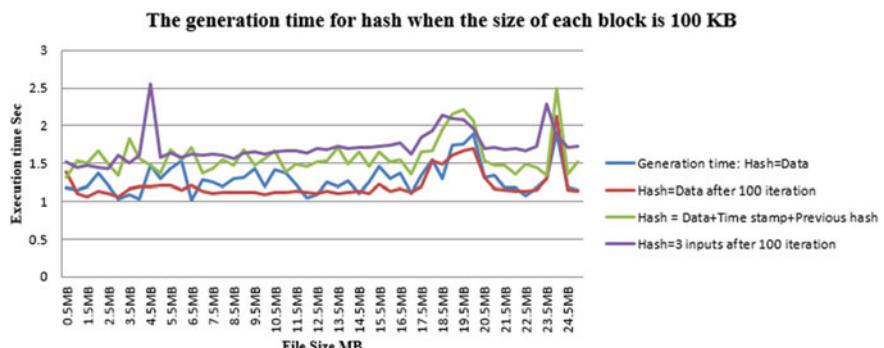


Fig. 21 The generation time for hash when the size of each block is 100 KB

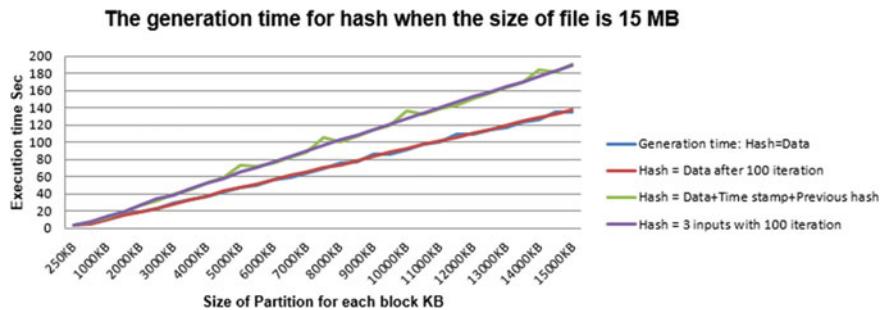


Fig. 22 The generation time for hash when the size of file is 15 MB

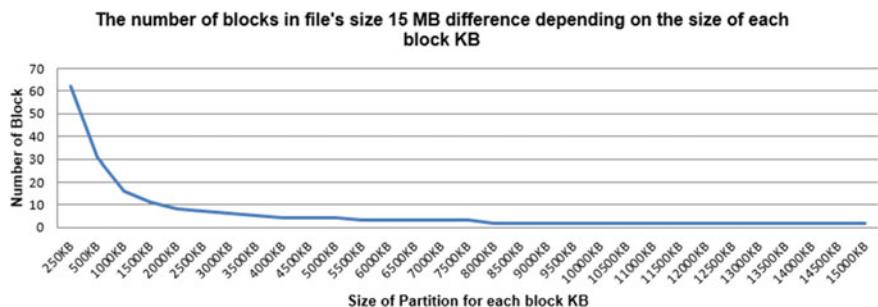


Fig. 23 The number of blocks in file size 15 MB difference depending on the size of each block KB

than about two MB, then the time of execution difference begins to increase as the block size increases. However, after several experiments, it was found that the time difference between the two methods does not exceed one minute, regardless of the size of the file, when choosing the ideal size for the block, which is: Block size = File size/2. The time at which the hash was created if it was created from data only or from previous data and hash and the time stamp, where the file size will be fixed (15 MB or 30 MB), and the hash size of each block in the chain will be variable, and we also show the difference in the number of blocks in each chain depending on the size of the blocks (partition), as shown in Figs. 22, 23, 24 and 25.

The number of blocks for a file (represents the number of records in the database for that file) represents the number of attacks that data can be exposed to, the more records there are, the more vulnerable they are to attackers, and vice versa, and therefore the data should be divided into the minimum number of blocks. The number of blocks of a file varies according to the size of each block and the size of the original file.

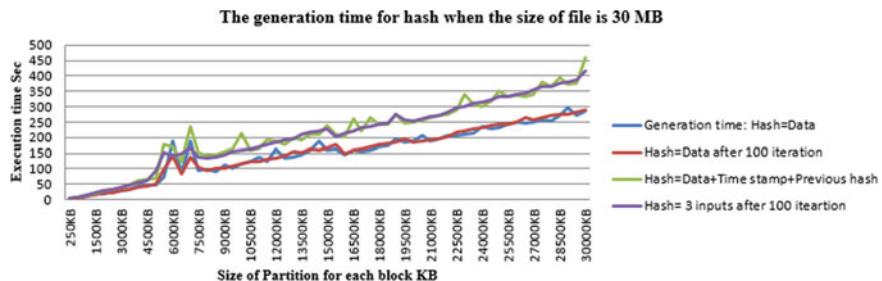


Fig. 24 The generation time for hash when the size of file is 30 MB

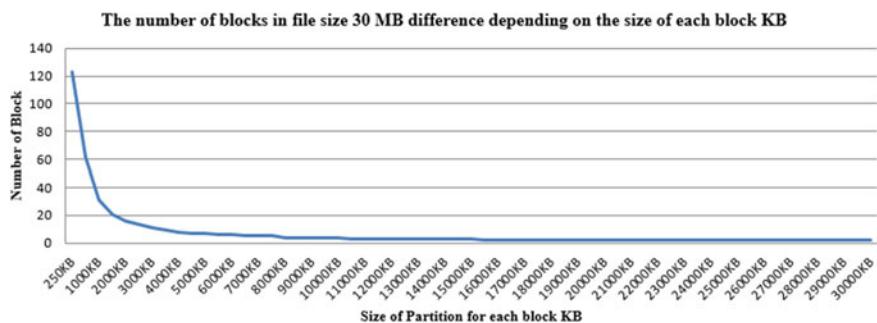


Fig. 25 The number of blocks in file size 30 MB difference depending on the size of each block KB

The increase in the size of the block means to decrease in the number of blocks representing the file and vice versa (inverse proportion).

Also, the increase in the size of the block (the size of the part to which the file was divided) means more time required to generate a hash and vice versa (proportional proportionality) and as we know the increased time of hash generation will effect on the performance.

Based on the focus on the two central issues (security and performance), and as a result of experimenting with several file sizes, it was concluded that the best block size is the file size divided by two, and at this block size, the number of blocks is the lowest possible, and the generation time of Hash is the least possible, and thus the required has been reached.

For example: If the size of the file is 30 MB, so the best size of the block is 15 MB, $30 \text{ MB} \times 1024 = 30,720 \text{ KB}$. So, the best size of block = $30,720 / 2 = 15,360 = 15 \text{ MB}$, the same thing we have noticed in the experiment.

Size of file is 30 MB = 30,720 KB

Size of block (KB)	Count of block	Size of block (KB)	Count of block
250	$30,720/250 = 122.88 = 123$	10000	$30,720/10000 = 3.072 = 4$
1000	$30,720/1000 = 30.72 = 31$	13000	$30,720/13000 = 2.363 = 3$
5000	$30,720/5000 = 6.144 = 7$	25000	$30,720/25000 = 1.22 = 2$

The same results that we obtained as a result of the experiment

The results demonstrated the ability of the proposed system to maintain data security at significant levels, in addition to its ability to overcome other types of threats:

1. A middle man attack (MITM):

The threat occurs between the two communication parties who are users and the cloud service provider CSP, where the intruder impersonates the other party to persuade the remaining parties to send messages to him directly in order to tamper with the data and steal it, but within our proposed system that attack will not succeed because the data had been encrypted via AES, As for key management using ECC, hijackers will not be able to return the encrypted data to its original form. In addition, authentication in blockchain technology between the two sides of the connection will achieve data integrity.

2. Distributed Denial of Service (DDoS):

Malicious Trojan horses use this attack to destroy system resources, this attack is very common, but through our proposed system that attack will not succeed due to the distributed blockchain architecture.

3. Cloud Service Provider (CSP):

CSP that stores data of the user will be able to view it and may use it for unauthorized purposes or even sell it to some other company without the customer's knowledge, so our proposed system consisting of mixed encryption algorithms will not allow the cloud provider to see the data because it will be in an unreadable encrypted mode, thus our goal in maintaining data security has been achieved.

Our proposed model that includes encrypting data in the SaaS layer and then sending it to data centers in IaaS layer that use blockchain technology will maintain data security and will ensure that:

- Confidentiality: via cryptography algorithms (AES, ECC), they have been used with the blockchain to ensure the security and confidentiality of data within the nodes of the chain so that no attacker can change the data, and thus no change on value for corresponding hash to protect against any penetration.
- Integrity: via hashing algorithms (SHA-256) in blockchain structure.

- Availability: via blockchain technology distributed decentralization.
- Performance: Faster, safer, and more efficient, because AES algorithm is the best, also ECC better than RSA.

Our proposed model provided 99% data security against all types of attacks, except for attack by using a quantum computer and a change of 51% of nodes peers' content.

Simulation and action were performed where the Android application was considered as the SaaS layer, and a local server was built as an alternative to the cloud so that it represents the IaaS layer, and to achieve decentralization in blockchain technology two databases were built, each one of them represents a node (ledger).

It should be noted that our results were recorded after 100 experiments as a benchmark to maintain the stability of our results, which may change as a result of changing the speed of the internet or the frequency of the processor's work. Another note: each attack on the chain is a modification of one of its blocks, thus the number of blocks modified in the chain is the same as the number of attacks. We assure that everything was built programmatically from the beginning without relying on something ready.

6 Conclusion

The rapid development and significant growth in the volume of data have led to the need for the concept of the cloud in our lives, and this need will increase further after the spread of the COVID-19 and the planet's transition to the virtual world. The security of data, confidentiality, integrity, and availability on-demand are always the most important factors that must be achieved to eliminate user anxiety in using the cloud. Traditional solutions such as cryptography only are no longer effective enough, so we have proposed a workaround that relies on a hybrid framework of AES algorithms for data encryption and ECC to distribute the keys and resist potential attacks in the SaaS layer, and, here, we have achieved the principle of data confidentiality, in addition to the presence of distributed blockchain technology in the IaaS layer creating more comfort for users, and, here, we have achieved data availability and integrity through authentication through the decentralized blockchain architecture. Thus, the requirements of cloud security (CIA) have been achieved and the data have become encrypted and distributed away from the threats. Our proposed framework has provided greater efficiency in terms of security with a rate of 99% and speed in implementation compared to previous studies.

References

1. Banafa A (2018) IoT and blockchain convergence: benefits and challenges. *IoT and blockchain convergence: benefits and challenges*. IEEE Internet of Things
2. Esposito C, Castiglione A, Martini B, Choo KKR (2016) Cloud manufacturing: security, privacy, and forensic concerns. *IEEE Cloud Comput* 3(4). <https://doi.org/10.1109/MCC.2016.79>
3. Modi C, Patel D, Borisaniya B, Patel A, Rajarajan M (2013) A survey on security issues and solutions at different layers of Cloud computing. *J Supercomput* 63(2). <https://doi.org/10.1007/s11227-012-0831-5>
4. Wang C, Liu X, Li v (2012) Implementing a personal health record cloud platform using CIPHERTEXT-policy attribute-based encryption. In Proceedings of the 2012 4th international conference on intelligent networking and collaborative systems, INCoS 2012, pp 8–14. <https://doi.org/10.1109/iNCoS.2012.65>
5. Zhang Q, Cheng L, Boutaba R (2010) Cloud computing: state-of-the-art and research challenges. *J Internet Serv Appl* 1(1). <https://doi.org/10.1007/s13174-010-0007-6>
6. Qian L, Luo Z, Du Y, Guo L (2009) Cloud computing: an overview. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol 5931. LNCS, pp 626–631. https://doi.org/10.1007/978-3-642-10665-1_63
7. Arutyunov VV (2012) Cloud computing: its history of development, modern state, and future considerations. *Sci Tech Inf Process* 39(3). <https://doi.org/10.3103/S0147688212030082>
8. Ramey J, Rao PG (2011) The systematic literature review as a research genre. <https://doi.org/10.1109/IPCC.2011.6087229>
9. Krishnan R (2017) ScholarWorks at WMU security and privacy in cloud computing. https://scholarworks.wmich.edu/masters_theses/919
10. Singh A, Chatterjee K (2017) Cloud security issues and challenges: a survey. *J Netw Comput Appl* 79. <https://doi.org/10.1016/j.jnca.2016.11.027>
11. Basu S et al (2018) Cloud computing security challenges & solutions-a survey. In 2018 IEEE 8th annual computing and communication workshop and conference, CCWC 2018, vol 2018. <https://doi.org/10.1109/CCWC.2018.8301700>
12. Sharma R, Trivedi RK (2014) Literature review: cloud computing –security issues, solution and technologies. *Int J Eng Res* 3(4). <https://doi.org/10.17950/ijer/v3s4/408>
13. Zhang R, Liu L (2010) Security models and requirements for healthcare application clouds. <https://doi.org/10.1109/CLOUD.2010.62>
14. Santos N, Gummadi KP, Rodrigues R (2009) Towards trusted cloud computing
15. Jansen W, Grance T (2012) Guidelines on security and privacy in public cloud computing?. In Public cloud computing: security and privacy guidelines, pp 1–95
16. Piliouras T et al (2011) Trust in a cloud-based healthcare environment. <https://doi.org/10.1109/CEWIT.2011.6135890>
17. Nyrönen et al TH (2012) Delivering ICT infrastructure for biomedical research. In ACM international conference proceeding series, pp 37–44. <https://doi.org/10.1145/2361999.2362006>
18. Bokhari MU, Shallal QM, Tamandani YK (2016) Security and privacy issues in cloud computing. In Proceedings of the 10th INDIACom; 2016 3rd international conference on computing for sustainable global development, INDIACom 2016, pp 896–900. <https://doi.org/10.5120/cae2017652617>
19. Bauer E, Adams R (2012) Reliability and availability of cloud computing
20. Hamdi M (2012) Security of cloud computing, storage, and networking. In Proceedings of the 2012 international conference on collaboration technologies and systems, CTS 2012, pp 1–5. <https://doi.org/10.1109/CTS.2012.6261019>
21. Iankoulova I, Daneva M (2012) Cloud computing security requirements: a systematic review. <https://doi.org/10.1109/RCIS.2012.6240421>

22. Bhushan K, Gupta BB (2017) Security challenges in cloud computing: state-of-art. *Int J Big Data Intell* 4(2):81. <https://doi.org/10.1504/ijbdi.2017.083116>
23. Toosi AN, Calheiros RN, Buyya R (2014) Interconnected cloud computing environments: challenges, taxonomy, and survey. *ACM Comput Surv* 47(1). <https://doi.org/10.1145/2593512>
24. Qevani E, Panagopoulou M, Stampoltas C, Tsitsipas A, Kyriazis D, Themistocleous M (2014) What can OpenStack adopt from a Ganeti-based open-source IaaS?. In IEEE international conference on cloud computing, CLOUD, pp 833–840. <https://doi.org/10.1109/CLOUD.2014.115>
25. Hashizume K, Rosado DG, Fernández-Medina E, Fernandez EB (2013) An analysis of security issues for cloud computing. *J Internet Serv Appl* 4(1):1–13. <https://doi.org/10.1186/1869-0238-4-5>
26. Ju J, Ya W, Fu J, Wu J, Lin Z (2010) Research on key technology in SaaS. In Proceedings-2010 international conference on intelligent computing and cognitive informatics, ICICCI 2010, pp 384–387. <https://doi.org/10.1109/ICICCI.2010.120>
27. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. *J Netw Comput Appl* 34(1):1–11. <https://doi.org/10.1016/j.jnca.2010.07.006>
28. Darwish MA, Yafi E, Almasri AH, Zuhairi MF (2018) Privacy and security of cloud computing: a comprehensive review of privacy and security of cloud computing: a comprehensive review of techniques and challenges. *Int J Eng Technol* 7(4.29):239–246. https://www.researchgate.net/profile/Marwan_Darwish4/publication/328927461_Privacy_and_Security_of_Cloud_Computing_A_Comprehensive_Review_of_Techniques_and_Challenges/links/5c4dcff9a6fdcc6b5cdedb/Privacy-and-Security-of-Cloud-Computing-A-Comprehensive-R
29. Dahbur K, Mohammad B, Tarakji AB (2011) A survey of risks, threats and vulnerabilities in cloud computing. <https://doi.org/10.1145/1980822.1980834>
30. Dawoud W, Takouna I, Meinel C (2010) Infrastructure as a service security: challenges and solutions
31. Kaaniche N (2014) La sécurité des données stockées dans un environnement Cloud , basée sur des mécanismes cryptographiques, p 201
32. Bhardwaj A, Subrahmanyam GVB, Avasthi V, Sastry H (2016) Security algorithms for cloud computing. *Procedia Comput Sci* 85:535–542. <https://doi.org/10.1016/j.procs.2016.05.215>
33. Yassein MB, Aljawarneh S, Qawasmeh E, Mardini W, Khamayseh Y (2018) Comprehensive study of symmetric key and asymmetric key encryption algorithms. In Proceedings of 2017 international conference on engineering and technology, ICET 2017, vol 2018, pp 1–7. <https://doi.org/10.1109/ICEngTechnol.2017.8308215>
34. Kulshrestha V, Verma S, Challa CRK (2017) A comprehensive evaluation of cryptographic algorithms in cloud computing. In Proceedings of the international conference on inventive computation technologies, ICICT 2016, vol 1. <https://doi.org/10.1109/INVENTIVE.2016.7823268>
35. Mahto D, Yadav DK (2017) RSA and ECC: a comparative analysis. *Int J Appl Eng Res* 12(19):9053–9061
36. Gilbert H, Handschuh H (2004) Security analysis of SHA-256 and sisters. In Lecture Notes Computer Science (subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol 3006, pp 175–193. https://doi.org/10.1007/978-3-540-24654-1_13
37. Ben Ayed A (2017) A conceptual secure blockchain based electronic voting system. *Int J Netw Secur Its Appl* 9(3):01–09. <https://doi.org/10.5121/ijnsa.2017.9301>
38. Wang S, Wang X, Zhang Y (2019) A secure cloud storage framework with access control based on blockchain. *IEEE Access* 7:112713–112725. <https://doi.org/10.1109/ACCESS.2019.2929205>
39. Park JH, Park JH (2017) Blockchain security in cloud computing: use cases, challenges, and solutions. *Symmetry (Basel)* 9(8). <https://doi.org/10.3390/sym9080164>
40. Kumar M, Singh AK, Suresh Kumar TV (2018) Secure log storage using blockchain and cloud infrastructure. <https://doi.org/10.1109/ICCCNT.2018.8494085>
41. 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. <https://doi.org/10.1016/j.dcan.2017.10.006>

42. Timothy DP, Santra AK (2017) A hybrid cryptography algorithm for cloud computing security. In 2017 international conference on microelectronic devices, circuits and systems, ICMDCS 2017, vol 2017, pp 1–5. <https://doi.org/10.1109/ICMDCS.2017.8211728>
43. Lin Q, Yan H, Huang Z, Chen W, Shen J, Tang Y (2018) An ID-based linearly homomorphic signature scheme and its application in blockchain. IEEE Access 6:20632–20640. <https://doi.org/10.1109/ACCESS.2018.2809426>
44. Zikratov I, Kuzmin A, Akimenko V, Niculichev V, Yalansky L (2017) Ensuring data integrity using blockchain technology. In Conference of open innovation association, FRUCT, vol 2017, pp 534–539. <https://doi.org/10.23919/FRUCT.2017.8071359>
45. Sukhodolskiy I, Zapecnikov S (2018) A blockchain-based access control system for cloud storage. In Proceedings of the 2018 IEEE conference of Russian young researchers in electrical and electronic engineering, ElConRus 2018, vol 2018, pp 1575–1578. <https://doi.org/10.1109/EIConRus.2018.8317400>
46. Rifi N, Rachkidi E, Agoulmene N, Taher NC (2018) Towards using blockchain technology for IoT data access protection. In 2017 IEEE 17th international conference on ubiquitous wireless broadband, ICUWB 2017-Proceedings, vol 2018, pp 1–5. <https://doi.org/10.1109/ICUWB.2017.8251003>
47. Raju S, Boddepalli S, Choudhury N, Yan Q, Deogun JS (2017) Design and analysis of elastic handoff in cognitive cellular networks. <https://doi.org/10.1109/ICC.2017.7996835>
48. Liang X, Shetty S, Tosh D, Kamhoua C, Kwiat K, Njilla L (2017) ProvChain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. <https://doi.org/10.1109/CCGRID.2017.8>
49. Puthal D, Malik N, Mohanty SP, Kougianos E, Yang C (2018) The blockchain as a decentralized security framework [Future Directions]. IEEE Consum Electron Mag 7(2):18–21. <https://doi.org/10.1109/MCE.2017.2776459>
50. Gajra N, Khan SS, Rane P (2015) Private cloud security: secured user authentication by using enhanced algorithm hybrid. <https://doi.org/10.1109/EIC.2015.7230712>
51. Liu L, Xu B (2018) Research on information security technology based on blockchain. In 2018 3rd IEEE international conference on cloud computing and big data analysis, ICCCBDA 2018, pp 380–384. <https://doi.org/10.1109/ICCCBDA.2018.8386546>
52. Saritekin RA, Karabacak E, Durğay Z, Karaarslan E (2018) Blockchain based secure communication application proposal: cryptouch. In 6th international symposium on digital forensic and security, ISDFS 2018-Proceeding, vol 2018. <https://doi.org/10.1109/ISDFS.2018.8355380>
53. Guo R, Shi H, Zhao Q, Zheng D (2018) Secure Attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access 6:11676–11686. <https://doi.org/10.1109/ACCESS.2018.2801266>
54. Esposito C, De Santis A, Tortora G, Chang H, Choo KKR (2018) Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. 5(1):31–37. <https://doi.org/10.1109/MCC.2018.011791712>

An Efficient Blockchain-Based IoT System Using Improved KNN Machine Learning Classifier



Roseline Oluwaseun Ogundokun , Micheal Olaolu Arowolo , Sanjay Misra , and Robertas Damasevicius

Abstract The introduction of blockchain technology (BT) has evolved into a distinctive, disturbing, and trendy technology in recent years. Data security and privacy are prioritized in BT's decentralized database. New security concerns raised by BT include common attacks and double-spending. To address the above-mentioned challenges, data analytics on a blockchain-based IoT network is necessary to protect data. The value of emerging technology Machine Learning (ML) is highlighted through analytics on this data. When ML and BT are combined, very precise results may be obtained. This study, therefore, aimed to give a comprehensive study on the use of machine learning to make Blockchain-based IoT network smart applications that are more robust to handle network attacks. To investigate these attacks on a blockchain-based IoT network, an improved K-Nearest Neighbor (KNN) classifier was postulated. Improved KNN (I-KNN) surpassed traditional KNN (T-KNN) with an accuracy of 96.7% and 81.6% for the I-KNN classifier and T-KNN, respectively.

Keywords Blockchain · IoT · K-Nearest Neighbor · Machine learning · Classification

R. O. Ogundokun · M. O. Arowolo

Department of Computer Science, Landmark University Omu Aran, Omu-Aran, Nigeria
e-mail: Ogundokun.roseline@lmu.edu.ng

M. O. Arowolo

e-mail: arowolo.olaolu@lmu.edu.ng

S. Misra

Department of Electrical and Information Engineering, Covenant University to Department of Computer science and Communication, Ostfold University College, Halden, Norway
e-mail: sanjay.misra@hiof.no

R. Damasevicius

Department of Software Engineering, Kaunas University of Technology, Kaunas, Lithuania
e-mail: robertas.damasevicius@ktu.lt

Abbreviation

ML	Machine Learning
BT	Blockchain Technology
KNN	K-Nearest Neighbor
T-KNN	Traditional K-Nearest Neighbor
I-KNN	Improved K-Nearest Neighbor
AI	Artificial Intelligence
DR	Detection Rate
FPR	False-Positive Rate
TP	True Positive
TN	True Negative
FP	False Positive
FN	False Negative

1 Introduction

Blockchain technology, the internet of things (IoT), and machine learning (ML) are now widely acknowledged as disruptive technologies with the ability to enhance present business procedures, establish novel business replicas, and disturb entire sectors. By offering a shared and decentralized distributed ledger, blockchain, for instance, could improve confidence, transparency, safety, and confidentiality in corporate operations. A blockchain, or a dispersed record in general, could hold all sorts of assets in the same way that a register can [1]. These data may primarily be linked to money and identities. IoT fosters industry automation and user-friendliness of business processes, both of which are critical for German and European industries. Finally, machine learning enhances processes by finding patterns and optimizing business outcomes [2]. Until now, the link between these three advancements has been overlooked, but blockchain, IoT, and machine learning have been employed in isolation. These advances, on the other hand, may and should be used in tandem, and they could be merged henceforth. A single probable link amid these technologies is that IoT gathers and distributes data, blockchain delivers framework and establishes engagement guidelines, and machine learning optimizes processes and rules [2, 3, 24]. These three inventions are complementary by design, and when coupled, they may fully realize their potential. The confluence of these technologies has the potential to be especially beneficial for data organization and the automation of corporate operations. Then, BT was mainly considered in the situation of payments, i.e., Bitcoin [4] and Ether (Bitcoin Cash). Non-financial applications of blockchain technology, for instance, supply chain management and digital identities, have evolved in recent years [5, 6]. The benefits of merging BT with other advancements like IoT and machine learning have been recognized in more recent research. Huh et al. [7], for example, highlight how blockchain technology might be used to advance the system

framework of IoT devices. Dorri et al. [8] describe how blockchain design may be changed to improve the infrastructure's ability to support IoT devices, particularly in terms of transaction speed. Some research focuses on the integration of blockchain and machine learning in addition to blockchain in conjunction with IoT [2]. Until now, the focus has been on linking blockchain with the two-revolutionary technology, which is IoT or machine learning, rather than implementing all three technologies at the same time. The actual potential of these new, developing technologies, however, will solitary be realized if they are merged. Kumar Singh et al. [9] propose a blockchain-based framework for IoT and machine learning. Unlike Kumar Singh et al. [9], their study presents a non-procedural review of all invention's advantages and in the way they accompaniment one another.

The widespread use of IoT devices is allowing different areas of our everyday life to be automated [10, 11]. The computerization of houses and cities, denoted as smart homes and smart cities, is one of the IoT's success stories [11]. Securing the transmitted and deposited data in the home system from malevolent activities wishing to cause havoc in someone's house is a big barrier to attaining the true vision of smart homes [12]. Although there are several competing technologies aimed at protecting data in smart homes from attacks, blockchain has developed as the utmost capable technology for both safeguarding the home network counter to data management attacks and offering a safe platform for the entire gadgets in the network to interact with one another during computation in the cloud (cloud computing) [13–15]. Considering the primary agreement protocols—a method by which the entire transactions are confirmed by the complete nodes—the data in a blockchain is immutable [16]. Administration attacks on conveyed or deposited data are therefore unlikely to succeed with a single hacked node, and a majority of nodes must be hacked [17]. Different consensus protocols are discussed, as well as their application to IoT networks [12, 18].

Without any examination, Gupta et al. proposed the idea of adding ML approaches to blockchain's consensus procedure as an impending study project [19]. The advantages of combining blockchain and artificial intelligence (AI) have been discussed by Dinh et al. [20]. They claim that a blockchain regulated by an ML algorithm may identify assaults and trigger appropriate protection measures or isolate the compromised component. This concept known as AI-enabled blockchain has been successfully designed and implemented (AIBC). Dey [21] presented a utility function for detecting anomalies [21] that is comparable to the function used in [17]. Then, he believes, this value may be fed into a supervised ML system to predict the likelihood of an attack and prohibit the consensus protocol's blockchain confirmation of that transaction. He does not, however, propose a strategy or implementation for creating a useful consensus protocol. They use Hyperledger fabric to create a 3-layer architecture to evaluate the validity of our 2-phase consensus protocol for IoT systems. The application layer, which houses various IoT devices, is the initial layer. The edge blockchain layer and the principal blockchain layer are the second and third levels, respectively, and contain various AIBC components.

To increase the accuracy of outcomes, data dependability and exchange are critical. The use of ML and BT together can produce extremely exact results. As a result, this study gives a thorough analysis of machine learning acceptance for making Blockchain-based IoT network smart applications further robust to attacks in this study. To investigate threats on a blockchain-based IoT network, an improved K-Nearest Neighbor (KNN) classifier is presented.

Numerous research works happen to address ML procedures for blockchain-based IoT applications; however, they have not yet been fully explored. In this study, the authors looked into the use of machine learning for blockchain-based IoT network smart applications. This paper's research contribution is listed below:

1. A quick look at how machine learning, the internet of things, and blockchain may be used to create smart application architecture.
2. To investigate threats on a blockchain-based IoT network, an improved K-Nearest Neighbor (KNN) classifier is presented.

The rest of the manuscript is prearranged as Sect. 2 discussed the material and method used for the execution of the study proposed classifier. Section 3 discussed the results discovered and the interpretation of the results. The paper was concluded in Sect. 4 and future work was also proposed as well.

2 Material and Method

This section discussed the datasets used for the execution of the system. The classifier employed for the execution and the performance metrics used for the study is discussed as well.

2.1 Datasets

The dataset used for the execution of the KNN classifiers is the IoT blockchain dataset. The dataset was downloaded from the Mendeley database repository. They consist of 17 features and 81 instances. The dataset can be found using this link: <https://data.mendeley.com/datasets/rxsdfg8ct9/1>. <https://doi.org/10.17632/rxsdfg8ct9.1>.

Bio studies: Supporting data is <http://www.ebi.ac.uk/biostudies/studies/S-EPM-C6412473?xr=true>.

2.2 Proposed System

A supervised ML classifier K-Nearest Neighbor (KNN) was used for the system execution. The IoT blockchain dataset was employed to assess the proficiency and

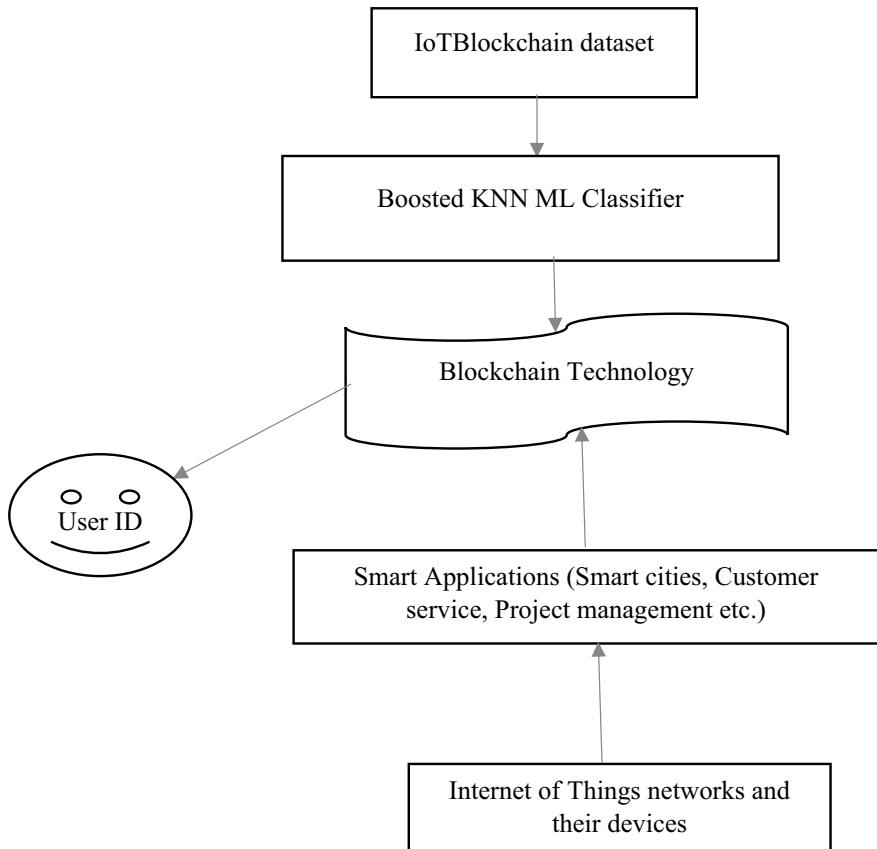


Fig. 1 Proposed I-KNN acceptance for Blockchain-based IoT network Smart applications

effectiveness of the projected classifiers which are T-KNN and I-KNN. After passing the dataset into the classifiers, the classification of the dataset was produced and these were evaluated using the confusion matrix performance analysis.

The proposed system architecture combining ML, Blockchain, and IoT systems was showed in Fig. 1. It was deduced that Blockchain technology is used to secure the system by authenticating the users of the system using their IDs. Blockchain technology is also used to secure smart applications and IoT networks.

2.3 Classification Evaluation

A confusion matrix was employed for the performance evaluation of the system executed. Accuracy, detection rate, and false-positive rate are the matrices used for the evaluation of the system. It can be deduced that a classifier effectively and

efficiently delivers a high accuracy and detection rate (DT) and a low false-positive rate (FPR). The formula of the three metrics are as follows [22]:

$$\text{Accuracy: } \frac{TP + TN}{TP + FP + FN + TN} \quad (1)$$

$$\text{DT: } \frac{TP}{TP + FN} \quad (2)$$

$$\text{FPR: } \frac{FP}{FP + TN} \quad (3)$$

3 Findings and Discussion

The results discovered and the interpretation of the results are discussed in this section.

3.1 Findings

Figure 2 displays the confusion matrix gotten during the execution of the T-KNN classifier while Fig. 3 displays the confusion matrix for the I-KNN classifier. It was discovered from the True Negative (TN), True Positive (TP), False Negative (FN), and False Positive (FP) values that the I-KNN outperformed the T-KNN classifier.

4 Discussion

The system's performance was assessed using a confusion matrix, which included parameters such as accuracy, detection rate, and false-positive rate. Accuracy and performance are both improved when the false-positive rate is reduced. In this work, the limitations of various approaches of accuracy, such as false-positive rates, are discussed [23]. Table 1 displays the confusion matrix for the classifiers, and Table 2 displays a comparison of the two classifiers used in this work, the T-KNN and the I-KNN. The I-KNN surpassed the T-KNN in terms of accuracy and FPR with an accuracy of 96.7% over 81.7% and an FPR of 0.048 over 0.22. The T-KNN surpassed the I-KNN in terms of DR with 100% over 97.4%, respectively.

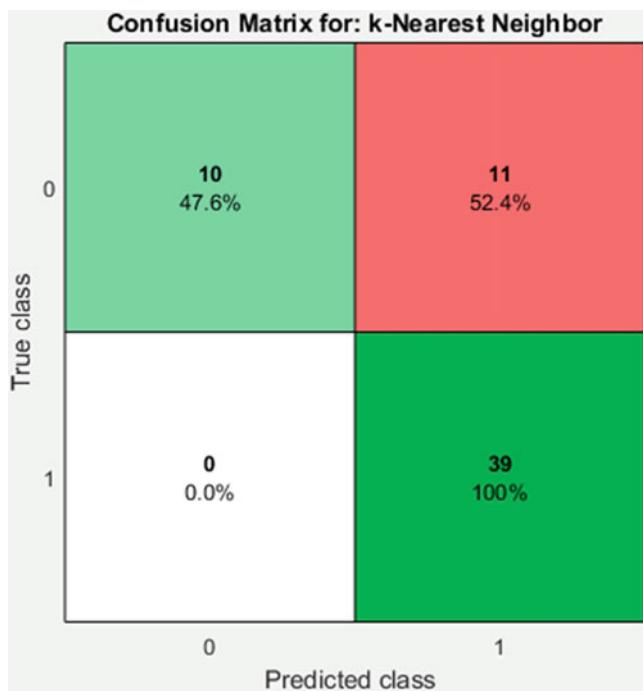


Fig. 2 Traditional KNN confusion matrix

5 Conclusion

Blockchain, the Internet of Things, and artificial intelligence most especially machine learning are all technologies that may be merged in many ways. It was contended that these advancements will converge because the combination of these technologies will boost business models, goods, and services. This study delivers a comprehensive study on the use of machine learning to make Blockchain-based IoT network smart applications more robust to attacks. To examine attacks on a blockchain-based IoT network, an improved K-Nearest Neighbor (KNN) classifier has been presented. With 96.7% and 81.6%, respectively, the improved KNN algorithm outperformed the traditional KNN method. Accuracy and performance are both improved when the false-positive rate is reduced. In this work, the limitations of various approaches of accuracy, such as false-positive rates, are discussed [23].



Fig. 3 Improved KNN confusion matrix

Table 1 Confusion matrix for the classifiers

Classifier	TP	TN	FP	FN
Traditional KNN	39	10	11	0
Improved KNN	38	20	1	1

Table 2 Comparative analysis between the classifiers

Measure	T-KNN	I-KNN
Accuracy	81.7%	96.7%
Detection rate	100%	97.4%
False-positive rate	0.22	0.048

References

1. Diedrich H (2016) Ethereum—Blockchains, digital assets, smart contracts, decentralized autonomous organizations. Wildfire Publishing, Washington, DC
2. Salah K, Rehman MH, Nizamuddin N, Al-Fuqaha A (2019) Blockchain for AI: review and open research challenges. IEEE Access 7:10127–10149. <https://doi.org/10.1109/ACCESS.2018.2890507>

3. Zheng P, Zheng Z, Wu J, Dai H (2020) XBlock-ETH: extracting and exploring blockchain data from ethereum. *IEEE Open J Comput Soc* 1:95–106. <https://doi.org/10.1109/OJCS.2020.2990458>
4. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. Available online at: <https://git.dhimmel.com/bitcoin-whitepaper/>. Accessed August 3, 2020
5. Treleaven P, Gendal Brown R, Yang D (2017) Blockchain technology in finance. *Computer* 50:14–17. <https://doi.org/10.1109/MC.2017.3571047>
6. Roeck D, Schönenseiffen F, Greger M, Hofmann E (2020) Analyzing the potential of DLT-based applications in smart factories. In: Treiblmaier H, Clohessy T (eds) *Blockchain and distributed ledger technology use cases—applications and lessons learned* (Cham: Springer), pp 245–266
7. Huh S, Cho S, Kim S (2017) Managing IoT devices using a blockchain platform. In: *Proceedings of the 19th international conference on advanced communication technology* (Piscataway, NJ: IEEE), pp 464–467
8. Dorri A, Kanhere S, Jurdak R (2017) Towards an optimized BlockChain for IoT. In: *Proceedings of the IEEE/ACM second international conference on internet-of-things design and implementation* (Piscataway, NJ: IEEE), pp 173–178
9. Kumar Singh S, Rathore S, Park JH (2020) BlockIoTIntelligence: a blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Gen Comput Syst* 110:721–743. <https://doi.org/10.1016/j.future.2019.09.002>
10. Adeniyi EA, Ogundokun RO, Awotunde JB (2021) IoMT-based wearable body sensors network healthcare monitoring system. *Stud Comput Intell* 2021(933):103–121
11. Olowu M, Yinka-Banjo C, Misra S, Oluranti J, Ahuja R (2019) Internet of things: demystifying smart cities and communities. In: *International conference on advances in computational intelligence and informatics*, pp 363–371. Springer, Singapore
12. Fernández-Caramés TM, Fraga-Lamas P (2018) A review on the use of blockchain for the internet of things. *Ieee Access* 6:32979–33001
13. Kazeem Moses A, Joseph Bamidele A, Roseline Oluwaseun O, Misra S, Abidemi Emmanuel A (2021) Applicability of MMRR load balancing algorithm in cloud computing. *Int J Comput Math Comput Syst Theory* 6(1):7–20
14. Lin J, Shen Z, Miao C (2017) Using blockchain technology to build trust in sharing LoRaWAN IoT. In: *Proceedings of the 2nd international conference on crowd science and engineering*, pp 38–43
15. Novo O (2018) Blockchain meets IoT: an architecture for scalable access management in IoT. *IEEE Internet Things J* 5(2):1184–1195
16. Dai Y, Xu D, Maharjan S, Chen Z, He Q, Zhang Y (2019) Blockchain and deep reinforcement learning empowered intelligent 5G beyond. *IEEE Network* 33(3):10–17
17. Salimitari M, Chatterjee M, Yuksel M, Pasiliao E (2017) Profit maximization for bitcoin pool mining: A prospect theoretic approach. In: *2017 IEEE 3rd international conference on collaboration and internet computing (CIC)* (pp. 267–274). IEEE
18. Salimitari M, Chatterjee M (2018) A survey on consensus protocols in blockchain for IoT networks. *arXiv preprint arXiv:1809.05613*
19. Gupta S, Sadoughi M (2019) *Blockchain transaction processing*. Springer International Publishing AG, part of Springer Nature 2018 Sakr S, Zomaya A (eds), *encyclopedia of big data technologies*, https://doi.org/10.1007/978-3-319-63962-8_333-1
20. Dinh TN, Thai MT (2018) Ai and blockchain: a disruptive integration. *Computer* 51(9):48–53
21. Dey S (2018) Securing majority-attack in the blockchain using machine learning and algorithmic game theory: a proof of work. In: *2018 10th computer science and electronic engineering (CEEC)*, pp 7–10. IEEE

22. Li Y, Chen Z (2018) Performance evaluation of machine learning methods for breast cancer prediction. *Appl Comput Math* 7(4):212–216
23. Narsingyani D, Kale O (2015) Optimizing false positives in anomaly-based intrusion detection using a Genetic algorithm. In: 2015 IEEE 3rd international conference on MOOCs, innovation, and technology in education (MITE), pp 72–77. IEEE
24. Gill SS, Tuli S, Xu M, Singh I, Singh KV, Lindsay D, ... Garraghan P (2019) Transformative effects of IoT, Blockchain and artificial intelligence on cloud computing: evolution, vision, trends and open challenges. *Int Things* 8:100118

Leveraging Blockchain Technology for Internet of Things Powered Banking Sector



Nayak Surekha , Rangasamy Sangeetha , Chellasamy Aarthy , Rajamohan Kavitha , and R Anuradha

Abstract Banking sector contributes to 70% of Indian Gross Domestic Product (GDP) and for India to meet its economic aspirations, it should enable this vivacious sector to grow at 8–10 times of its current pace, in the next ten years. This pace of active growth requires a double engine of sophisticated technology and a tech enabled, scalable, and a secured banking system. Implementing Blockchain Technology (BCT) in the banking sector, provides a realistic solution which when coupled with devices connected by the Internet of Things (IoT), will result in secured, fast-paced, cost effective, and transparent growth of the sector. The prevalence of personalized banking, secured banking, connected banking, and digital banking are use cases, made possible through interface with IoT. This chapter delves into the opportunities in the banking sector to be explored and challenges to be met in the BCT-IoT implementation process. BCT- and IoT-based opportunities such as peer-to-peer lending, Know Your Customer (KYC) updation, Cross-border transfer payments, syndicate lending, fraud reduction are some of the banking operations that are elaborated. To strengthen the banking network, the consensus algorithm of Blockchain network is much required and the use of IoT devices to act as nodes is pertinent. The blend of both in the banking space has to be further reinforced.

N. Surekha · R. Sangeetha () · C. Aarthy · R. Anuradha
School of Business and Management, CHRIST University, Bangalore, India
e-mail: sangeetha.r@christuniversity.in

N. Surekha
e-mail: surekha.nayak@christuniversity.in

C. Aarthy
e-mail: aarthy.c@christuniversity.in

R. Anuradha
e-mail: anuradha.r@christuniversity.in

R. Kavitha
School of Sciences, CHRIST University, Bangalore, India
e-mail: kavitha.r@christuniversity.in

Keywords Blockchain technology · Internet of Things (IoT) · Smart contract · Swoc (strength weakness opportunities and challenges) analysis · Banking

1 Introduction

At 2030, I would say that you probably have two billion people that will be using day to day banking services, independent of banks—Brett King

Digital Transformation across the globe has disrupted all the industries, specifically the banking sector put up in second place behind telecommunication [1]. The underlying reason for this transformation is Fintech industries with new market entrants challenging mainstream markets [2]. Competitive atmosphere along with customer expectations forced the banks to focus on product and service innovations that led to a global rise of cashless payment. This is further driven by supportive policies from the government, changing consumer behavior, and ease of use of technology. Presently, the banking sector is in a situation to adapt to new digital ecosystem by leveraging new digital technologies like Blockchain Distributed Ledger Technology, Crypto currencies, IoT, Application Programming Interface (API), Artificial Intelligence and Analytics thereby reinventing themselves and focusing customer-driven enterprises [3]. The plunge for digital payment arises from technology companies and e-commerce giants such as Google, Apple, Facebook, Amazon (GAFA). The ongoing pandemic has made it inevitable to shift to a safe and secured blockchain enabled contactless payment system. Global digital payment methods can be done through Unstructured Supplementary Service Data (USSD), Aadhaar enabled Payment System (AePS), Unified Payments Interface (UPI), Mobile Wallet, Bank Prepaid cards, Point of sale (PoS), Internet banking, mobile banking and Micro-Automated Teller Machine (ATM). Thanks to strong two-factor authentication, people believe that risk and fraud are less and countries like Sweden (Mobile BankId) allows consumers to authenticate with a few finger taps for digital payments. According to the Reserve Bank of India (RBI)[4] in 2019 the volume of financial transactions through UPI has surpassed credit or debit card transactions. In this space of digital payments another innovation is to move from P2P (Purchase to Pay) payments to C2B (Consumer to Business) and B2C (Business to Consumer). App-based payment gateways such as Tikkie & MobilePay are testimonies for such services where customers get paid faster through Whatsapp irrespective of whom they bank with.

The need for short-term financing has brought into the forefront concepts such as “Pay Later” and “Customer Credit Offering” that has garnered huge attention in emerging Asian markets especially in India and China. Pay Later is a system wherein the consumer does not pay a fee or interest, instead the merchant does it and Customer Credit Offering is where the customer pays interest and the merchant is free of charge [5]. Machine Learning (ML) and Artificial Intelligence (AI) are integrated with pay later solutions which help the lender to verify credit worthiness and background check at a faster rate with low risk. According to a study by Boston

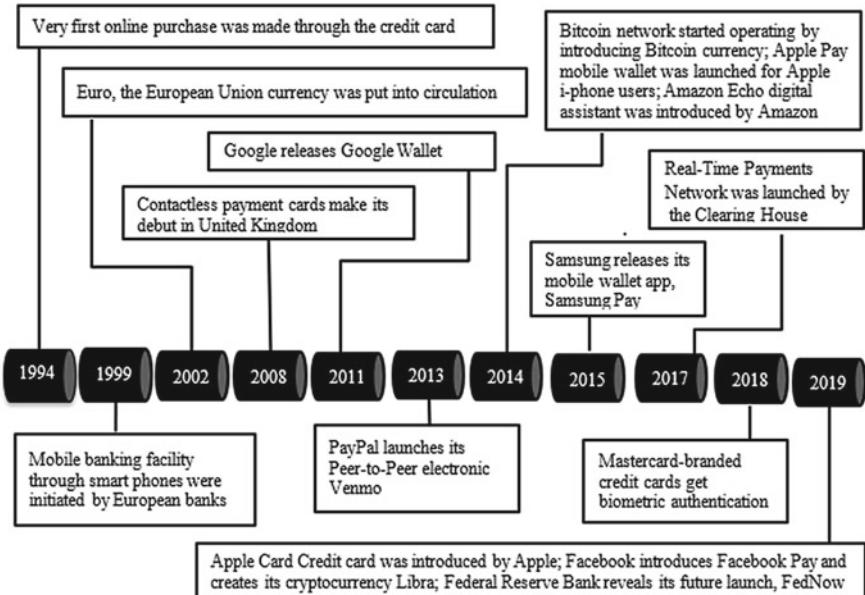


Fig. 1 Milestones in digital payments

Consulting Group (BCG) [6] 82% of global enterprises have expressed their interest in adopting IoT solutions for their payment with an expected market reach of USD 267 billion by 2020. Currently there are IoT streamlining payments such as GPay, Amazon Pay being connected at home with various smart devices. Evidence traced from Visa study [7] hints that though 83% of global consumers are willing to use connected devices for transactions, 75% of people step back due to security issues. Digital payments can be referred to as monetary transactions that take place using any smart device which is seamlessly connected with a bank account. Research from Statista [8] expects a six-fold increase in global digital payments from \$532 billion to \$3100 billion in next six years. Figure 1 depicts the timeline of milestones achieved in digital payments. Such tremendous growth is an outcome of business models developed by tech companies in collaboration with banks, payment companies, and social networking platforms [9].

Industry 4.0 propelled technologies such as IoT, AI, ML is not only confined to the manufacturing sector but equally benefits the service sector contributing to a high share of GDP in advanced economies [10]. Banking sector, being the lifeline of digital society, robust technology needs to be initiated to ensure transparency. Decentralization being a key feature in blockchain enhances transparency, removes intermediaries by not emphasizing on third-party validation [11] and augments the business process [12]. Blockchain embedded with IoT gives a cognitive sense to objects which bridges the gap between the digital and physical world thereby enhancing automation through interconnected devices. IoT when amalgamated with Blockchain can

exchange the data through sensors thereby avoiding third-party authentication which achieves cost efficiency, reduces risk, increases processing speed, and ensures trust by creating a valuable business model [13]. This chapter aims to provide the readers with detailed information on blockchain technology enabled IoT for the banking sector. It describes the various applications of IoT as connected solutions in the banking space and discusses the status of blockchain implementation by commercial banks in India. Finally the strength, weakness, opportunities, and challenges (SWOC) of implementing Blockchain in banking is discussed.

2 Application of IoT in Financial Services Sector

IoT is a novel and growing technology that creates a network of a variety of things or devices such as mobile phones, sensor embedded smart devices, and Radio-Frequency Identification (RFID) tags. IoT is designed in a variety of applications where people, devices, and firms are involved to provide connected solutions such as connected health, connected home, connected vehicle, and connected banking. Figure 2 shows the applications of IoT in the financial sector.

The combination of the IoT and financial services is a fast developing trend. In the financial sector, the IoT technologies are used to monitor assets, understand customer behavior, promote payments through wearable devices, fraud alert, improve investment and visibility of the capital market, and enhance the customer experience. The Global IoT Market is predicted to grow from \$150 billion in 2018 to \$1.5 Trillion by 2025 [14]. The IoT establishes the digital connectivity between customer and the bank/ financial institution for anything, anytime and anywhere. In the financial sector, the IoT technologies are used to personalize customer service, improve decision-making, gather data in real time, and enable smart interaction with customers. The involvement of IoT in different financial services is discussed in the following subsections.

2.1 Banking Sector

IoT is not only a concept, it is a real time, technology enabled network of devices and customers. In recent decades, there has been a greater evolution in electronic devices and software industries which leads to increasing the usage of IoT devices from millions to billions. Exclusive IoT softwares developed for the banking sector has resulted in drastic changes by way of new facilities such as retail banking, connected banking, personal Banking, digitized banking, secure banking, and mobile banking as depicted in Fig. 3.



Fig. 2 Applications of IoT as connected solution

Retail Banking

Digital acquaintance of customers who use smart mobile, smart watch, card reader, tablet, and laptop has made the banking sector adopt IoT-connected devices and technologies for better user experience and cost reductions. This has facilitated the wide usage of Smart Automated Teller machines (ATM) resulting in reduced transaction time. A digital ecosystem of IoT-connected wearable devices such as apple watch and fit pay enables banks to recognize their potential customers and their business needs. It also supports banks to gain customer insights, provide value added services, and suggest financial assistance.

Connected Banking

Banking sector uses chatbots for efficient interaction with their customers to provide personalized experience. These chatbots are developed using machine learning with Natural Language Processing (NLP). The IoT with chatbot facilitates 24/7 customer

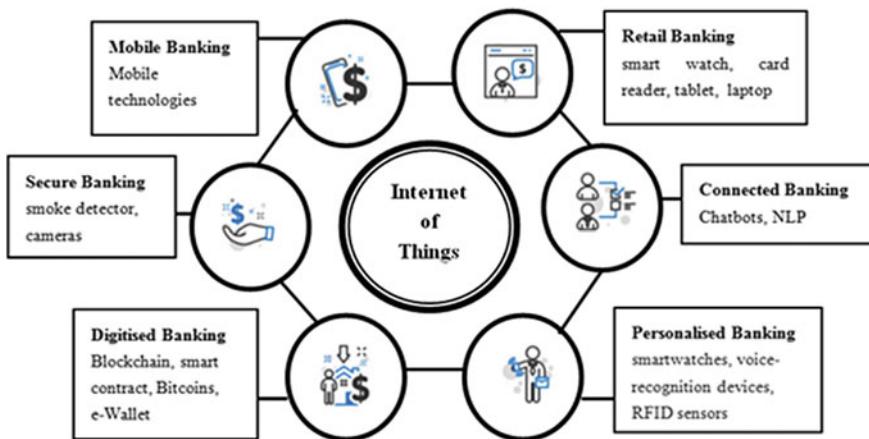


Fig. 3 IoT concepts and devices in banking sector

support for everyday banking needs such as account balances, spending analysis, budget recommendations, location-based suggestions, and transaction history. The authors [15] discussed the role of chatbot in the banking sector for customer services. Natural Language Processing incorporated chatbot application gives a unique feel to the customer by personalized response in user friendly manner. Also they mentioned that the chatbot application creates strong social relationships and emotional bonds with the customers.

Personalized Banking

The IoT-connected devices are used to alert the customers based on their financial habits and help them to avoid overspending. Recently, IoT enabled banks introduced shock wearable devices to customers which monitors their spending habits and alerts by a shockwave when they reach the credit limit. This mechanism prevents the customer from overspending. Data stored in IoT devices such as credit history will enable banks to sanction loans and design products to suit customer needs. Also, wealth management companies can procure insights on a real-time basis to plan personalized investment portfolios. Bluetooth beacons are widely used to aid special-needs customers to navigate branches and meet their needs.

Digitized Banking

IoT enabled blockchain technology provides better authentication in terms of privacy and security since the created credentials are not possible to be changed or altered. The blockchain technology makes cross-border payment easy and trade finance more efficient. Digitalization of banks provides more agility in terms of first-mover advantage and flexibility in adopting innovative technologies such as bitcoins, contactless payments, and digital Wallet. These forward thinking banks provide customers with mobile and internet banking services providing value for time and convenience.

Secure Banking

Deployment of security systems with a set of sensors like smoke, cameras, and IoT technologies prevent the bank from unpredictable accidents and theft. In addition it helps in monitoring suspicious activities by customers or intruders and alert the concerned authority. However during the transaction, data related to bank and customer transmitted via the IoT network is vulnerable to leaks and breaches. This recommends absolute benchmarking by banks providing such facilities.

Mobile Banking

Mobile banking allows its customers to make financial transactions using mobile devices like smartphones and tablets. Mobile banking services can be via mobile applications or through short message services (SMS). Mobile apps allow the customers to check balance, history of the transaction , and loan statements. This also provides other services like fund transfers, locating ATM and bank branches, registering and tracking the complaint, and cancelling an issued cheque. SMS-based mobile banking allows customers to enquire about their account balance and block credit/debit cards along with cheques when stolen or compromised.

2.2 Insurance

IoT is looking to revamp the process of many businesses including the insurance domain. Most of the companies are in the process of shifting from paper-based manual systems to automated and digitized systems. The type of insurance namely, automotive insurance, health insurance, life insurance and home insurance can gain immense benefits from the significant data being generated from millions of connected devices such as sensors, wearable devices, and smartphones which are used by customers. The following subsections outline application of IoT in the insurance domain.

Automotive Insurance

Connected vehicles are manufactured with a set of sensors to measure and transmit data like cornering, mileage, speed, and location. Initially the collected data is used to get the driver's action and performance but in later stages this valuable information helps to understand the impediment risk for insurance firms. Data collected from well-established IoT connected cars are fed into AI to get real-time pre-analyzed details of automotive insurance customers. The industry experts believe that in automotive insurance, IoT data creates more opportunities in leveraging and staying competitive. It also helps to promote and maintain smart connected automotive insurance. So, the insurance firm uses the combination of telematics and AI algorithms to reduce the chances of accidents, control fraud and develop competitive insurance products.

Home Insurance

The usage of connected IoT devices in the home environment is increasing due to multiple benefits. The sensors adopted in the smart home of the customers generate

a stream of data which can be used by home insurance companies to contemplate on future challenges and mitigate them. IoT technology in home automation prompts insurance companies to avoid false and high priced claims thereby maintaining stability between return on capital investment and customer benefit. Thus insurance companies use apt combo marketing techniques such as purchase of IoT devices like Canary-a device to detect intruders, Cocoon AI-smart security camera and Ring-a smart video doorbell and discount on home insurance products.

Life Insurance

The IoT-connected wearable devices like fitness tracker and smart watches are used to monitor the policyholders. Newly introduced PAYL (Pay-as-You-Live) products are connected with the wellness of the customer thereby bringing in continuous interaction and promoting more insurance products. For instance, if a customer is traveling a temporary travel insurance is suggested. The policy holders are monitored and rewarded with benefits like discounts in gym membership and organic products. Normally life insurance policies are declined to the people who have health issues. These people can benefit by a policy with a regular underwriting approach. UK-based insurance company, Exeter, introduced the product "Managed Life" to the consumers with type-2 diabetes [16]. This product is possible with real-time tracking using connected IoT devices.

Health Insurance

IoT embedded medical devices, also known as wearables, have created a tremendous change in the healthcare industry. These devices are used to observe parameters like pressure and sugar level in the blood and pulse rate. The inclusion of wearable devices into health insurance provides robust benefits to insurers and their consumers. The data provided by the wearables gives the view on their consumer's lifestyle and health condition which enables the insurers to provide personalized solutions with financial benefits. IoT wearable manufactures, health care providers, and insurance companies are jointly working to provide budgetary real-time data capturing mechanisms with AI for remote health monitoring. This monitoring system helps the health insurance companies to lessen their claims by suggesting incentives to their policyholders.

3 Blockchain and IoT for Banking

Blockchain is a type of data structure used in Distributed Ledgers (DL) that stores and transfers data from a block which is connected through a digital chain. Blockchain uses cryptographic and algorithmic methods to record and match the data across the network. DL is a shared record of transactions among the participants/nodes in the network and. DL can be either permissioned or permissionless based on the rights given to the network participants to alter the database with or without the permission of a validator. It also can be public or private depending on the right given to the participants to access the ledgers. For example, a new digital currency transaction can be recorded and shared to a network of blockchain and once it is validated by

Table 1 Technicalities, legalities, and economic aspects of smart contracts

Technical aspects	Economic aspects	Legal aspects
Auto verification	Transparent	Automated processes
Enforced execution	No central authority	Enhanced security
Immutable	Less of transaction cost	Assurance of Governance

all the participants in the network, it will be added to the existing blockchain. Since it is validated and added to the blocks in a linear mode, earlier blocks cannot be altered or modified by the participants. Distributed Ledger Technology (DLT) has been related to digital currency since 2008 when the inventor of Bitcoin Satoshi Nakamoto described it as “an electronic payments system based on cryptographic proof instead of trust, allowing any two interested parties to transact directly with each other without the intervention of a trusted third party” [17]. The requirement of a trusted third party is to avoid double spending issues. Digital currency can be spent twice by an individual well versed with the concept of blockchain. Hence to overcome the double spending issue cryptographic elements were introduced by enhancing security and integrity in a DL which are maintained through the network of connected devices. Apart from the currency based blockchain there are smart contracts based blockchains too. Smart contracts facilitate automation of compliances in various industries including governance and provide smooth flow of operational processes. Table 1 presents the underlying aspects governing smart contracts.

Following are the steps involved in developing a smart contract:

1. Define the various processes involved in and develop Standard Operating Procedure
2. Each event to be automated with the requirement/checklist.
3. Execute and transfer the required documents with digital signatures.
4. Settlement
 - On chain (Digital).
 - Off chain (Physical).

4 Status of Blockchain Technology Implementation by Commercial Banks in India

Despite the fact that blockchain technology is in its nascent stage it is capable of revamping the existing process and exploring new services. This technology has the potential to disrupt the banking domain, specifically cross border payments, automated banking ledgers, and digital assets [18]. A report on “Ease of Doing Business” by the World Bank ranked India at 63rd position (2020)from 73 (2015) which is a phenomenal growth by leveraging technology and rationalizing regula-

tory requirements [19]. It also states that E-Governance in India faces challenges in terms of scalability, diversity, and complexity in the delivery of various public services and blockchain can address these issues and improve e-governance service. In recent years, India has successfully laid the foundation for digital infrastructure which eases blockchain implementation thereby having better control in contract management and decentralization of authority in decision-making. Finance industry is witnessing a massive surge in BCT applications aiming to improve operational efficiency and customer experience. An Indian community called Bankchain was established in 2017 to reduce fraudulent activities and improve information sharing. This community has 37 members including public, private, and international banks along with technology companies [20]. India is also a forerunner in experimenting adaptation of BCT in trade finance, cross-border payments and loyalty and digital identity [21]. ICICI Bank along with Emirates NBD launched a BC-based network EdgeVerve, developed by Infosys, to aid international trade finance and remittances. The framework supports the features like distribution, extensible, and permissioned blockchain [22]. Mahindra group of companies and IBM developed cloud-based blockchain supporting supply chain financing to improve transactions between supplier and manufacturer. The Proof of Concept worked better for invoice discounting, a method that enhances invoicing process. Mahindra Finance is also exploring the use of the shared ledger concept for small and medium-sized enterprises loans [21]. Bajaj Electricals in tie up with Yes bank is using smart contracts in vendor supplier financing, thereby reducing paperwork and processing time from five days to real-time basis. Using a permissioned or closed-loop BCT framework system ensures that only pre-registered and authenticated users carry out transactions. Axis and Kotak Mahindra Bank (KMB) are testing BCT transactions focussing on cross-border remittance and trade settlements. KMB has partnered with JP Morgan Singapore to use BC in issuing letters of credit for outbound and inbound transactions. In 2018 Infosys has invited ICICI Bank, Axis Bank, Kotak Mahindra Bank, Yes Bank, IndusInd Bank, RBL Bank, and South Indian Bank to test trade finance transactions on BCT Experiments are in progress by Deloitte India in blockchain-based customer rewards and loyalty [21]. and by National Stock Exchange (NSE) to view values in post-trading settlements, CKYC (Central Know Your Customer) services, trading voice exchanges, and invoices. Thus BCT implementation has advantages to the sector in terms of enhanced security in transactions and facilitating low cost cross-border transactions [23]. Though various processes are involved in smart contract implementation, this chapter concentrates only on KYC, Trade Finance, Cross-border payments, Syndicate lending, Credit rating, and Reduction of bank frauds which is mentioned as Fig. 4.

4.1 *Know Your Customer (KYC)*

Trust being the foundation of the Banking sector, identity verification of a customer is a prerequisite. Earlier, verification and validation of customer details were through

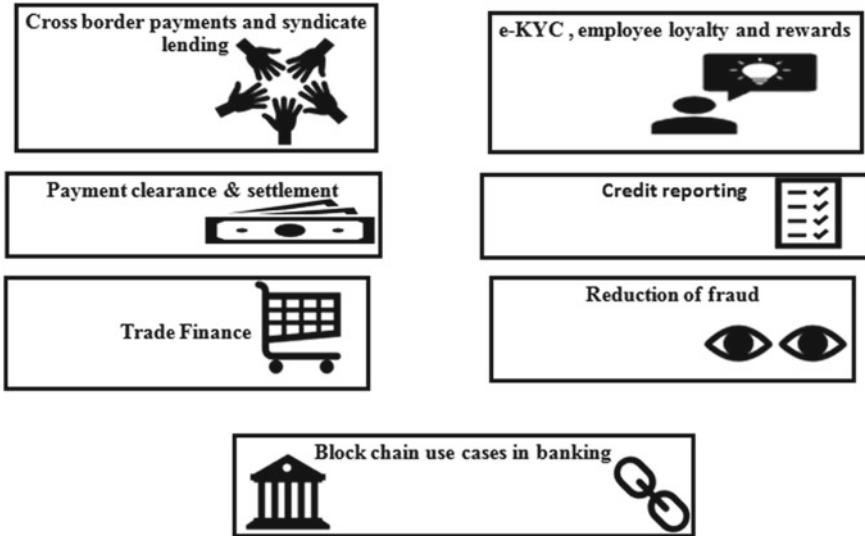


Fig. 4 Use cases of Blockchain in Indian banking sector

time consuming physical channels which were later digitized due to IoT. However, this created data safety concerns as the customer's data stored by way of email accounts, credit card details, and network passwords became vulnerable and prone to hacking. This fuelled the need to adopt BCT in KYC processes. The urgency was also felt as KYC was expensive and time consuming along with being a regulatory compliance. Based on Thomson Reuters survey, 2017 [24], KYC procedures are required on an average 32 days as compared to 26 days during 2016. KYC processes starting with digital identity, records a set of attributes that includes name, birth date, gender, and nationality of an individual or a set of information related to an entity used by computer systems to represent an external agent [25]. Regulators impose huge demands on the bankers to comply with Anti-Money Laundering (AML) and KYC regulatory requirements. Once KYC is carried out, the details are stored digitally and are assigned with a unique identification number for each customer. This identification number can be used whenever the customer approaches for a new service within the same bank or with other banks. Having a secure e-ecosystem is an essential criterion for the banks planning to adopt BCT as it will substantially lower security issues by enabling an individual with a digital identity. The embedded feature of cryptography is an added advantage that secures shared data and is kept in a central repository called distributed ledger. This is accessible by all financial institutions. Blockchain along with IoT applied for KYC processes will enhance the interoperability among bankers globally, reduce administrative costs, and avoid duplication of data thereby facilitating reduction in infrastructure cost [26]. These advantages motivated several banks to adopt the R3 enterprise blockchain platform (Corda) to implement blockchain for the KYC process [27]. Reference [28] in their

research work suggested that permissioned blockchain can be used for customer privacy protection in the public “KYC Smart Contract” and private “KYC Admin Smart Contract”. The former takes into account blockchain operations like CRUD (Create, Read, Update and Delete) to approve participants/customers whereas the latter is responsible for adding the KYC file to the repository, Inter Planetary File System. The combination of public and private smart contracts provides both, free access in the Public phase and enables restriction through encryption in the Private phase. Public portion of the smart contract allows organizations and syndicates across the globe to participate in a secure environment through permissioned blockchain with customers worldwide. Following are the processes involved in creating an encrypted KYC database through the implementation of Blockchain along with IoT.

1. Users/participants/customers across the globe can connect through IoT and access KYC User Interface for user registration.
2. Once the registration is approved user can submit required documents which will be processed in Decentralized IPFS (Inter Planetary File System).
3. Livelihood and survival mobility are oftentimes outcomes of uneven socioeconomic development.
4. Once the documents meet the requirements, the evaluator will approve the user for registration.
5. Dedicated KYC services process will be initiated through quorum permissioned blockchain where two-step processes are embedded.
6. There will be an evaluator (external entity) to scrutinize the KYC document.
 - a. KYC Smart Contract (CRUD—Create, Read, Update and Delete operations are available for the approved users).
 - b. KYC Admin Smart Contract—All the details of the approved users are stored with UID which can be accessed only with the private key to make it more secure and immutable.

Point 1 to 6 explains the KYC process. Once this process is completed, the UID can be referred to by the customer/user or any individual whenever the user approaches any financial institutions for any services worldwide. Following are the steps involved in using the UID for further transitions.

1. The customer should share the public key with the banker with whom a financial transaction is initiated.
2. The banker will access the database using the public key and add an OTP to the user’s public key.
3. The OTP will be shared by the banker to the customer through SMS.
4. The customer will use the OTP along with his private key to decrypt the personal data and validate his/her identity using digital signature.
5. Validation by the customer through digital signature signifies that the KYC verification process is successful.
6. There will be an evaluator (external entity) to scrutinize the KYC document.

Hence the implementation of IoT enabled Blockchain will enhance the effectiveness of KYC processes. Distributed Ledger Technology (DLT) will help augment the real-time approval of financial documents along with faster processes. While appreciating the advantages that are brought in by Blockchain enabled IoT one cannot forget the infrastructure challenges, Scalability challenges, and Security issues.

4.2 *Trade Finance*

Finance arrangements made by the parties involved in a trade are called trade finance. Trade can be domestic or cross-border, involving exporters, importers, banks, shippers, insurers, and government agencies. Generally international trade is paid in advance, so the majority of the trade amount is financed through banks. Buyers' expectation of on time delivery of quality merchandise and sellers' expectation of prompt payment has given rise to various intermediaries to strike a balance. Even though payment mechanisms such as telegraphic transfer, open account, payment by delivery, and letter of credit are in place, letter of credit is considered as a secure and effective trade financing mode. Letter of Credit as a payment method involves the following steps.

1. Buyer prepares a purchase order in consultation with bank buyer.
2. Bank Seller issues the invoice
3. Buyer applies for Letter of Credit (L/C)
4. Approval and sharing of L/C by buyer to bank buyer and bank buyer to bank seller
5. Seller prepares the goods on the receipt of approval and L/c
6. Seller handovers the goods to shipper along with the trade document Bill of lading (B/L)
7. Seller sends the B/L to Bank seller
8. Bank seller sends the B/L to Bank buyer
9. Bank buyer confirms the receipt of B/L to buyer
10. Buyer initiates the payment
11. Bank buyer transfers the payment to bank seller
12. Bank seller credits the account of the Seller
13. Buyer presents the B/L to the claim the goods
14. Shipper delivers the goods and transfer of ownership leading to the end of the transaction.

These cumbersome processes have pain points like creation of manual contract, factoring of invoice, delay in timeline, reviewing the Anti-Money Laundering (AML) requirements, miscommunication, multiple entries of bills of lading, and delay in payment. This necessitates a smart contract to be executed by the parties involved in trade finance. Blockchain based Distributed Ledger System through Smart contract makes the trade finance processes more efficient and effective. The benefits reaped

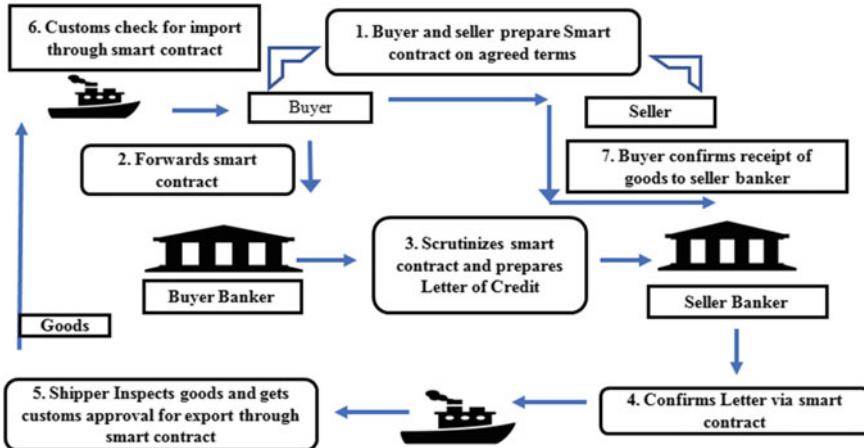


Fig. 5 Trade finance process enabled with IoT and Blockchain

are in terms of real-time review and approval, trusted intermediary, short-term factoring services, proof of ownership, automated settlement mechanism, reduction in transaction time and cost along with transparency in regulatory compliance. Figure 5 illustrates the processes involved in trade finance which can be embedded with smart contracts. The manual processes depicted with 14 steps are reduced to 7 through blockchain technology.

Enabling trade finance with Blockchain based smart contracts provides simplification of operations, connects all the parties involved in trade finance real time, manages the processes relating to letter of credit effectively leading to automated settlement.

4.3 Financial Market Infrastructure (Payment, Clearing, and Settlement)

The growing reliance on the financial sector by individuals and business houses has magnified the importance of the banking sector in an economy. The banking ecosystem has evolved and has advanced due to the enormous volume of transactions done on a daily basis and the complicated mesh of interconnected networks. The banking function of payments, clearing, and settlements is one such complicated area with substantial daily volumes that needs to be securely monetized by multiple parties. Determining the obligation is termed as clearing, and discharging the obligation is called settlement. It is a way of off-setting mutual monetary claims and obligations between entities through regular non-cash payments with subsequent transfer of the balance [29]. The logical solution for reducing this evolving ecosystem's complexities is the blockchain technology enabled IoT system boosted by the 5G mobile

network standards. IoT and BCT eliminate a substantial chunk of manual processes and bring in place 'smart contracts' that enable monetization of transactions accurately and at real-time speed, thereby simplifying the whole process. 5G enabled IoT speeds up the process involved in clearing and settlements, and Blockchain technology bestows the advantage of securely validating such transactions, thereby incorporating the "trust" factor through its distributed consensus and cryptography features. This makes both these technologies complementary to each other [30]. IoT devices can fill in for the requirement of participating nodes in blockchain required for consensus, while blockchain technology can mitigate the IoT's security issues. Thus, the banking sector needs to upgrade its business strategy by adopting private blockchain technology to streamline the clearing and settlement process. Adopting BCT will weed out the requirement of a third-party intermediary, the clearinghouse, and enable speedy peer-to-peer settlement leading to a massive reduction in costs of settlements. A typical clearing and settlement bank transaction will take on an average a few days if done traditionally due to the limitations posed by the existing financial infrastructure and the complicated system of intermediaries, but involving the blockchain technology will reduce the time to few seconds with the added advantages of reduced costs, impenetrable security and accompanying secured documentation. Clearing and settlement systems essentially include the transfer of assets between parties. When IoT is adopted, these physical assets are converted into digital assets. However, the main drawback is that the owner of a physical asset can show the asset and prove his ownership before he intends to transfer it to the other party, whereas in the case of digital assets, an individual can claim ownership for an asset which he does not own and create multiple copies of digital data that he had owned in the past. Traditionally, this limitation is addressed by appointing a central authority to maintain and overlook the data that is authenticated to transfer the ownership of data when transfer requests arise. If there are more parties involved, then there arises a need for some mechanism to be in place that connects their database and syncs it. Nevertheless, the threat of data security breaches remains, and also the time taken for completing the transaction will be in days. The solution to this is to enable IoT through BCT, wherein all the participants individually and remotely control their nodes and execute the decided steps to update their respective ledgers, which are interlinked. When new transaction requests crop up that necessitate a change in the ledger, each participant will verify the transaction and authenticate it according to the consensus protocol rules. In the blockchain setup, every participant will own a public key and a private key in pairs. The private key will be used to sign a transaction, and the rest of the participants will then use their public key to verify the transaction which helps the participant justify that they indeed signed the transaction. The ownership of data on a blockchain is associated with an address. The public key gets this address through the hashing mechanism and includes additional bits to it. The participant proves his ownership of the address by signing the transaction with the private key. Thus, the transactions are authenticated and are pooled into a block. When new transactions come in, they get authenticated and added to the block through the consensus algorithm. Figure 6 details the IoT-based Clearing and Settlement System mechanism through the application of BCT.

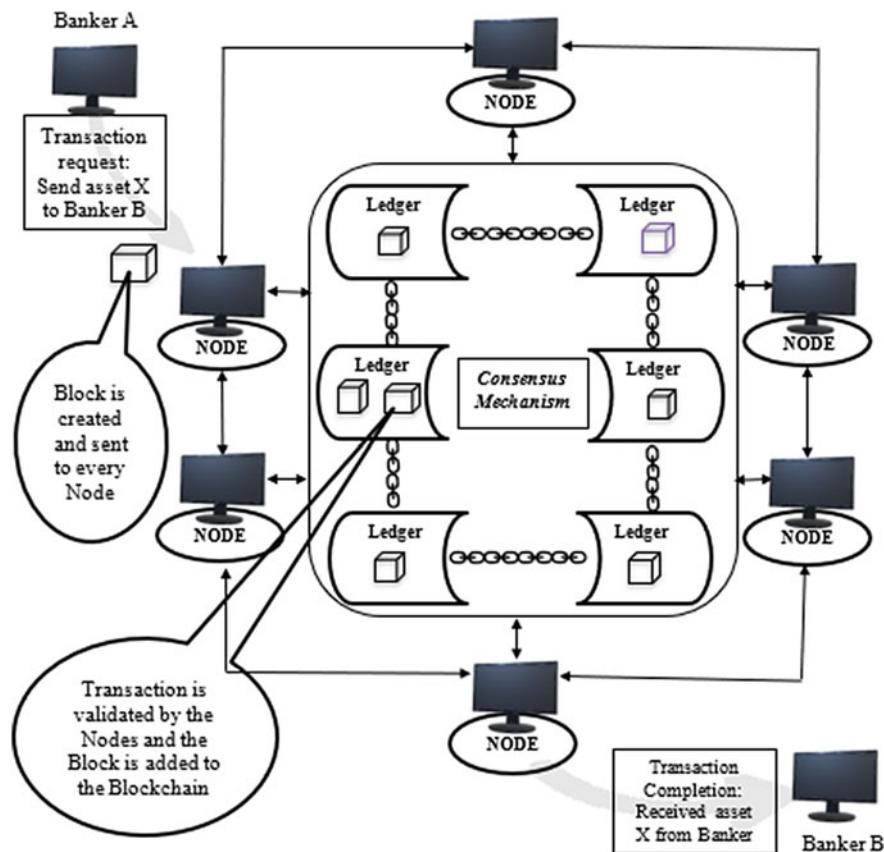


Fig. 6 IoT-based clearing and settlement system powered by Blockchain

4.4 Peer to Peer (P2P) Bank Transfers and Cross Border Payments

IoT has changed the way transactions are carried out in the banking space, the most notable one being the peer-to-peer transfers that enable account holders to transfer funds from their respective bank accounts or credit cards to another using an online banking or mobile banking app. The process for such a transfer is simple with the sender logging in to his/her net banking or mobile app and entering the details that include the name of the sender, amount to be transferred, debit/credit card details, and security PIN, thereby confirming the transfer. With such a fast and reliable process, the ease of making money transfers has increased multifold, but P2P transfers have built-in limitations that substantially reduce their effectiveness. These limitations include restriction of operations to a narrower geographical location, longer transaction time which ranges from one to three business days, data security issues,

and fraud, to name a few. The system gets even more complicated when the payments involve different currencies affected by the exchange rates, multiple banking regulations, costly currency conversions, international transfer fees, and other related costs. However, these limitations can be removed in their entirety and the whole process can be secured and completed in real-time by incorporating blockchain technology. Having a reputation of being a universal ledger existing in a distributed network that is accessible to all the participants, blockchain maintains a complete record of all the transactions. It keeps them permanent and immutable through a consensus mechanism where all the participating nodes validate the remittances. The whole process eliminates the need of intermediaries who pose a threat of dilution of security and data breach and increased costs. The Peer-to-Peer (P2P) Bank transfer mechanism more or less works in the same way as the clearing and settlement mechanism.

4.5 Credit Reporting

A credit report is a document that conveys data about an individual's credit history and includes information relating to the person's identity, information received by credit reporting agencies as to the credit standing, and publicly documented information such as bankruptcy reports. These reports need to be accurate since any mistake, or falsified information in the report will lead to wrong decisions resulting in heightened credit risk for the banks dealing with the individual. The amount of decisions a bank takes in terms of managing its retail credit portfolio is enormous and includes decisions relating to the acceptance/rejection of loan application, authorizing the over-limit, actions to be taken for default cases, identifying accounts that would possibly default, and cross-sell/up-sell strategies. This necessitated automation in the lending space which considerably reduced manual work in terms of paper work and the associated costs leading to the advent of Credit Reporting Systems. It includes credit bureaus, credit reporting companies operating on a commercial basis, and credit registries. They build a database that stores information related to the debtors. Nonetheless, the main threat in Credit reporting Systems, similar to other banking services, is data leakage. To secure a safe spot for credit reporting in the banking ecosystem, BCT has to provide the technical foundation for the Credit Reporting System which will remove the need for credit reporting intermediaries and strengthen the system by making it immutable through smart contracts. Creating a common credit report ledger by implementing BCT and including all the approved banks and financial institutions as participants of the ledger will ensure single version and accurate information being deciphered among the participants and ensure the safety of the data. On similar lines, a shared identity management ledger created through the blockchain system that involves government departments, educational institutions, banks, and financial institutions as participants will resolve the identification problem and make this sensitive data immutable as shown in Fig. 7. Sophisticated algorithms attached with the BCT can help bring credibility factors to identity management by validating the borrower's unique identity and garner credit information of a particular

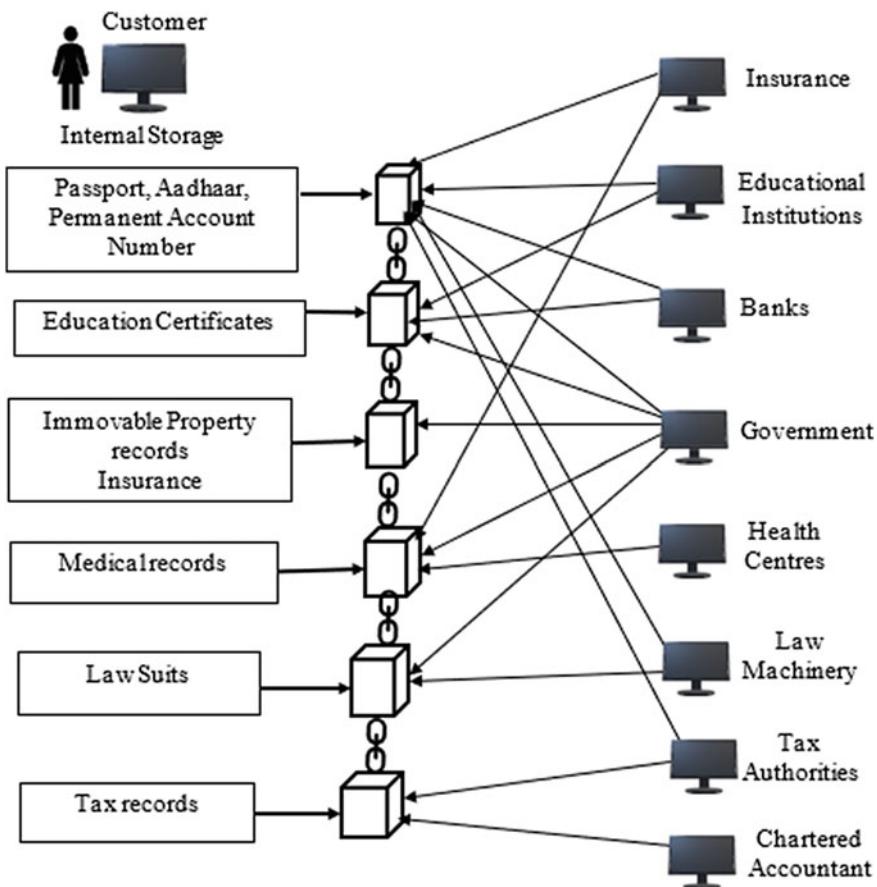


Fig. 7 BCT enabled shared identity management ledger system

borrower over the years. The consumer's data protection is also ensured since the customer, whose information needs to be accessed, will grant access to the required data by using the private key.

4.6 Reduction of Fraud

Unlawful appropriation of any property including money with the intention of deceiving others is called fraud. If such frauds are committed on the internet, it is called cyber fraud. The banking industry is prone to malicious damages in fraud and cyber-attacks that have raised many concerns in the recent past ever since the industry embraced IoT that surged the banking activities into digital mode. Currently prevail-

ing centralized ledger systems where personal and financial data related to customers are stored has been the target of hackers and fraudsters. Banking frauds related to technology-based services in the retail banking arena include identity theft, fraud in documentation, e-banking (related to debit card and credit card) theft, multiple funding, Card Not Present (CNP), incorrect sanctions, internet banking fraud, and ATM fraud. Corporate banking frauds are in terms of asset stripping, siphoning of funds, diversion of funds, frauds in documentation, over-valuation of collaterals, and non-existence of collaterals. The most recent addition to this list of frauds is where the core banking system is compromised. When Society for Worldwide Interbank Financial Telecommunications (SWIFT) [31], which is the payment processing system is compromised, the fraudsters gain the advantage of arbitrarily transferring funds to remote accounts since SWIFT is the gateway that allows fund transfer to connected financial institutions. The ever-growing number of payment systems currently available in the market place also multiplies the risk of frauds associated with it. However, the spike in the number of frauds over the years is more in retail banking as it is process and volume-based compared to corporate banking. The limited availability of resources in terms of human resources and technology to monitor the processes, verifying the documents, and incomplete customer information has made banks vulnerable to fraudsters. Figure 8 depicts a BCT-based credit report management system.

Figure 9 projects the sheer increase in value of payments and clearing transactions of the growing Indian economy through the years 2017–18–2019–20. The payment and settlement systems captured a robust growth rate in 2019–20, expanding by 44.1 per cent in volumes on top of the growth by 55.8% in the year 2018–19. In value terms, the increase is by 5.4% when compared to 14.2% of the previous year due to reduced growth in the Real Time Gross Settlement (RTGS) system. During the year 2019–20, the portion of digital transactions as a part of the total non-cash retail payments increased to 97% as compared to 95.4% in 2018–19. However, the digital transactions were hard hit due to the ongoing COVID—19 pandemic that caused a downturn in the economic activity and lowered discretionary payments [32]. At the global level the total payments revenue stood at \$1.9 trillion in the year 2018[33]. On the other hand, bank frauds too rose substantially. The annual report of Reserve Bank of India (RBI) reveals that the bank frauds of rupees one lakh and above amounted to 71,543 crore in 2018–19 while it stood at 1.85 trillion in the year 2019–20 with a whooping 159% increase. In terms of volume, the total fraud increased from 6,799 in 2018–19 to 8,707 in 2019–20 registering a 28% increase [32]. As evident from the above-stated figures, as banks move toward embracing emerging technologies like IoT in their everyday transactions, the cases of bank frauds are also increasing. One of the effective preventive mechanisms the banking industry can look up to is blockchain technology. If IoT is intertwined with BCT, these fraudulent activities can be significantly reduced and the sensitive data can be guarded diligently. BCT enables a decentralized storage mechanism and puts a consensus mechanism in place, which will prevent hackers from gaining effortless access to the stored information. The process of Smart contracts also ensures the safety and accuracy of transactions since each of the previous steps of a transaction is linked with the consecutive step

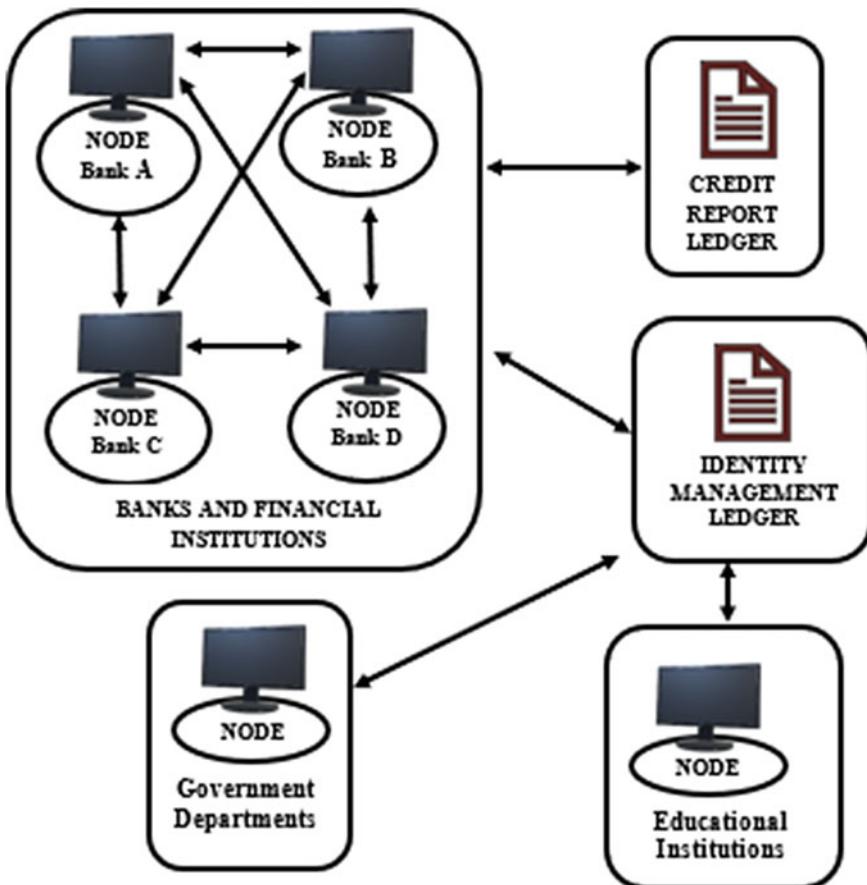


Fig. 8 BCT enabled identity management and credit report management systems

through hashing, and as such, the transaction cannot be completed if it is not in sync with the previous step, resulting in a foolproof method of transacting.

4.7 *Loan Process*

The lending platforms of banks are ever busy since a considerable amount of transactions fall under the retail lending category. Typically, the loan funds available under the umbrella of retail loans include housing loans, consumption loans for durable commodities, car loans, education loans, personal loans, and credit cards. The loan values of these retail lending are increasing multifold.

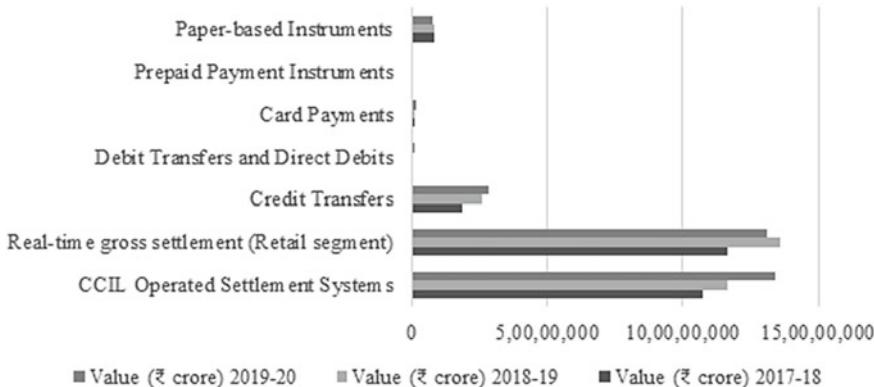


Fig. 9 Value of transactions (annual turnover) processed by payment systems in India (2017–2018 to 2019–2020) [32]

4.8 Syndicated Lending

Traditionally, the banks have a typical workable model for lending, where the banks originate loans and portray them in their balance sheet, which exposes them to risk and incentivizes the banks to screen and monitor borrowers [34]. However, this system proved to be cumbersome due to banks' ever-increasing customer base, which necessitated an alternative model to reduce such risks. The resultant system was "syndicated lending", which led to the massive development and growth of the syndicated loan market, which was further boosted by IoT's introduction over the past two decades as shown in Fig. 10. Syndicated lending permits a bank (known as the Originating bank or the Lead bank) to originate a loan. However, it gives the advantage of retaining only a fraction of such loans and selling the remaining part to a syndicate of investors consisting of banks and institutional investors, thereby sharing the credit risk across the syndicate. Other benefits that accrue to the Lead bank due to syndicated lending are that the lead bank receives interest in its share of loan and gets a fee for arranging such syndication. Also, it reduces the work of screening credit risk and monitoring the borrowers. On the other hand, institutional investors get to participate directly in funding the loans originated by the banks rather than funding the banks themselves. Syndicated loans dominate the marketplace even today and have paved the way for a booming international syndicated lending market. The amount of work involved in this process is enormous. The instrument in itself is complex with a gamut of detailed provisions, elaborate regulations that borrowers need to comply with, changing terms of repayment, involvement of multiple currencies, revolving credit facilities, to name a few. Besides, each Lead bank might be involved in a portfolio with hundreds of loans outstanding at different stages of their respective credit periods. As such, the syndicated loan system poses itself as the right candidate to be enabled through BCT.

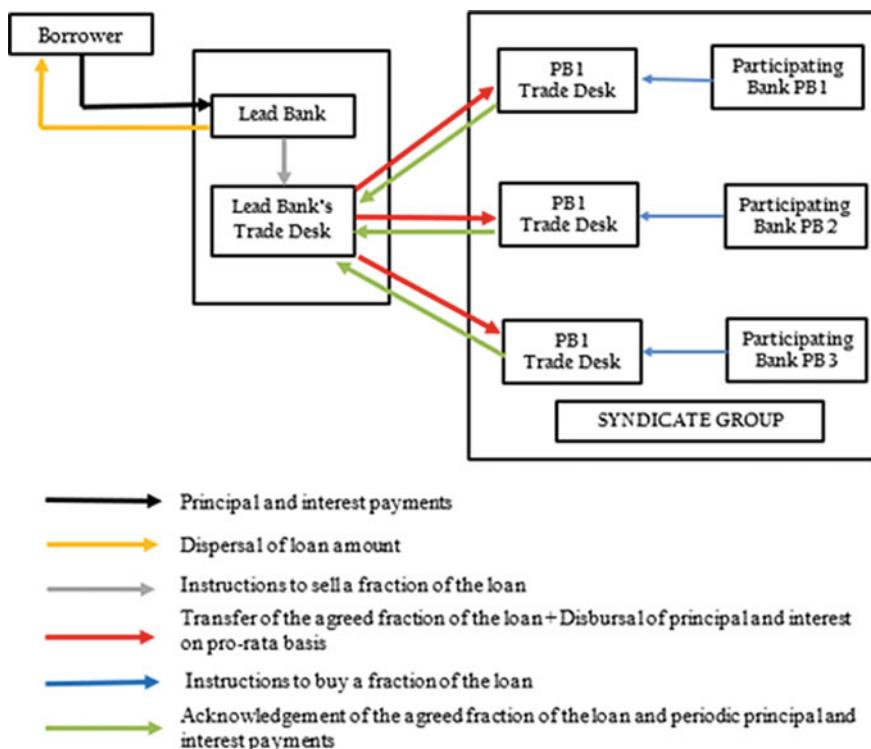


Fig. 10 Loan syndication system without Blockchain technology

As depicted in Fig. 10, the whole system is simplified by the adoption of BCT. Since the same contractual terms apply to all the syndicated group participants, BCT will eliminate the need for each of the participants to maintain its records. A shared ledger is maintained through the consensus mechanism wherein all the participants' computers (nodes) are connected to this shared ledger. The ledger preserves past transactions and is open to audit at any point in time. It also offers utmost security through the digital signature mechanism, which authenticates the participant who transacted, thereby weeding out the need for the elaborate KYC norms. The modus operandi of digital signature is already explained in detail in the previous Sect. 4.1 of this chapter. BCT also mitigates the requirement of a regulator, thereby easing out the whole process. The above discussion on various areas where BCT can be adopted effectively in the banking industry proves that the technology is ready to revolutionize the industry if implemented along with the IoT. It creates a secured environment that is system resilient and automates the entire banking process. It not only increases the trust factor among the participants but from a technical viewpoint, will also help the participants improve the quality of data, provide absolute control of the data, and protect it from tampering. BCT will secure the transactions from the security angle through the process of distributed ledger, consensus algorithm,

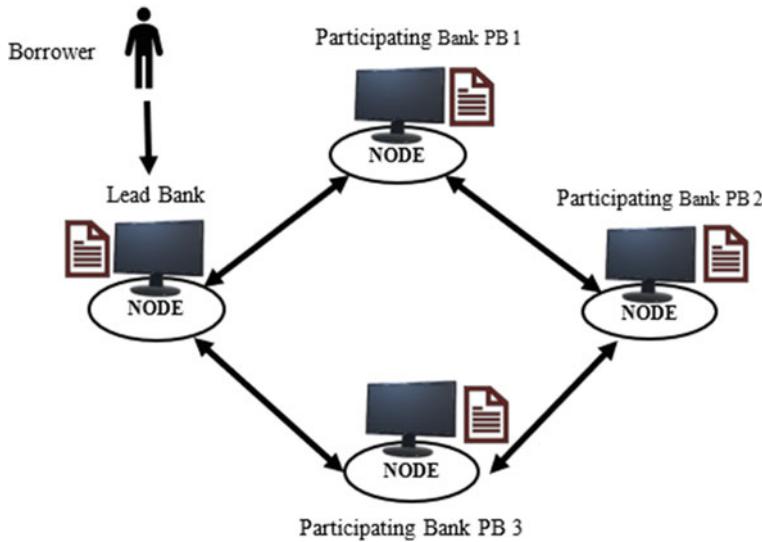


Fig. 11 Blockchain technology enabled loan syndication system

and smart contract, thereby reducing frauds and fraudulent transactions. From the operations point of view, BCT will improvise the record-keeping system, speed up the settlement process, reduce human intervention, eliminate time lag, reduce error, and weed out unnecessary third parties, thereby lowering operational, financial, and transaction costs. BCT also takes care of the regulatory compliance and renders the transactions to immediate audit by the participants. Governance-wise, BCT offers a maximum advantage in terms of immutability and tractability. Layering BCT with IoT will streamline the business process and provide real-time speed in communication and transactions as shown in Fig. 11.

5 SWOC (Strength Weakness Opportunities and Challenges) Analysis on Blockchain Technology in Banking

Technological development over the years along with the emergence of the internet impacted the banking sector tremendously. No one can deny the convenience, speed, efficiency, effectiveness, and transparency technology has brought into the banking sector [35]. Competitive atmosphere along with customer expectations forced the banks to focus on product and service innovations. The advent of internet finance also has posed multiple challenges in the traditional banking businesses. Internet finance is perceived as a boon due to the four important characteristics namely conducive payment infrastructure; multiple service integration, multi-channel integration, and

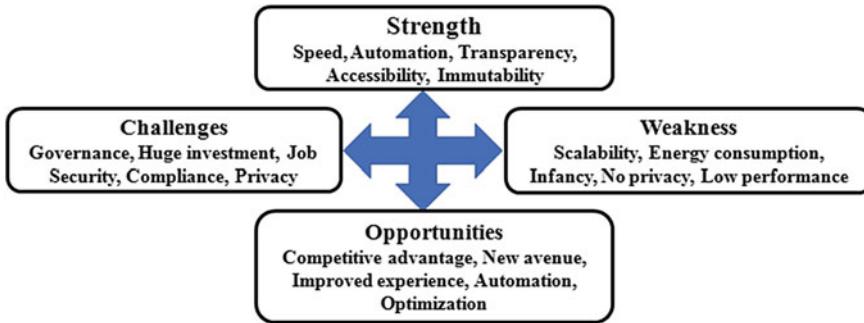


Fig. 12 SWOC analysis of IoT and BCT in the banking industry

various application scenarios [36]. “A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by the consensus of a majority of the participants in the system. Once entered, information can never be erased. The Blockchain contains a certain and verifiable record of every single transaction ever made” [37]. However various risks such as technical risk, technology risk, operational risk, legal risk as well as regulatory risk involved in the implementation of blockchain technology is a matter of concern [38]. Being a disruptive technology, Blockchain technology has an immense impact on finance and banking industry with the conception of Bitcoin. Bitcoin being a permissionless blockchain technology has been widely used by several countries for the payment of goods and services. Yet one needs to understand the underlying challenges involved in permissioned blockchain technologies such as Ripple [39]. Based on the above discussions about application of blockchain technology enabled IoT in the banking sector, SWOC analysis is presented in Fig. 12.

6 Conclusion

Banking sector has evolved to what it is today due to major technological changes that this industry has adopted. From manual maintenance of accounts to computerized accounts to e-passbooks, MICR cheques to Internet transfer of payments, cheque clearance centers to NEFT/RTGS, introducer to a bank account to eKYC, queueing in the banks to no physical existence of branches and m-banking, the evolution is ongoing. Banking sector is the backbone of Indian Financial System and it is imperative that this strong system is reinforced without compromising on safety and privacy of customers’ data and hard earned earnings. Blockchain technology is making itself felt in the banking sector as an indispensable force in data management and transparent money transfer. The integration of Blockchain technology into the banking domain is inevitable and it is the responsibility of the research-industry-

Central bank trio to make this integration seamless with proper checks and balances. Technological innovations always come with errors and compatibility issues and through continuous research and development, the issues of scalability, privacy, and security can be resolved. Promising fintech companies in technical collaboration with blockchain technology specialists are already taking this one step ahead with several chatbot managed branches, chatbot financial advisory services, asset management for various risk levels and many more. When research provides many new technologies, industry acceptance of the technology is pertinent to bridge the gap between technology and its users. The consortium of India's eleven largest banks, including Yes bank, South India bank, ICICI, Kotak Mahindra bank have built the first ever blockchain linked loan system and is a testimony of the faith reposed by Indian banking system on the new technology. Use of blockchain technology for streamlining the process for digital identity, cross-border payments, KYC updates, and credit rating evinces the implementation of technology along with IoT. The integration of servers, providing accessibility on a real-time basis, multiple device based operation of accounts have made banking very simple, cost effective, and popular. Riding through the internet wave, the central banks have consistently provided a regulatory framework for several banking operations enabled via the internet. In similar lines, the regulatory framework for full fledged banking operations, which performs beyond mere storage of customer data on blockchain, will be provided by the Central bank, is the anticipation and hope. Once the sub-systems of fool proof technology for payments transfer, accessibility of customer data by banks all across globe to prevent duplication of customer information, transparency through scalable proof of work algorithm, high digital percolation and access to high-speed uninterrupted internet, are in place, the final application of Blockchain and IoT in Indian banking sector will successfully happen.

References

1. Schepinin V, Bataev A (2019) Digitalization of financial sphere: challenger banks efficiency estimation. In: IOP conference series: materials science and engineering, vol 497. Institute of Physics Publishing. <https://doi.org/10.1088/1757-899X/497/1/012051>
2. Diener F, Špaček M (2021) Digital transformation in banking: a managerial perspective on barriers to change. *Sustainability (Switzerland)* 13(4):1–26. <https://doi.org/10.3390/su13042032>
3. Rohan, Sounak (2019) Future of digital payments. Infosys. Retrieved from <https://www.infosys.com/services/digital-interaction/documents/future-digital-payments.pdf> Accessed on 7-4-21
4. Singh JB (2019) Annual report 2018-2019. Reserve Bank of India. Retrieved from: <https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs>. Accessed on 23-6-2021
5. AnaPatravanu (2019) Invoice and pay later solutions-trends updates and innovation. In: Payment methods report 2018–2019, p 144
6. Hunke N, Yusuf Z, Rüßmann M, Schmieg F, Bhatia A, Kalra N (2017) Winning in IoT
7. Webster K (2017). Consumers want new IoT ways to pay. payments.com. Retrieved 6 23, 2021, from <https://www.pymnts.com/internet-of-things/2017/visa-and-pymnts-research-the-future-of-online-payments-and-iot-connected-devices-for-consumers>
8. Statista (2019) Fintech report 2019-digital payments. <https://www.statista.com/study/41122/fintech-report-digital-payments/>

9. Müttel S (2021) Unlocking the payment experience: future imaginaries in the case of digital payments. *New Media Soc* 23(2):284–301. <https://doi.org/10.1177/1461444820929317>
10. Mariani M, Borghi M (2019) Industry 4.0: a bibliometric review of its managerial intellectual structure and potential evolution in the service industries. In: *Technology forecasting social change*. <https://doi.org/10.1016/j.techfore.2019.119752>
11. Aarthy C, Aishwarya N (2019) An outlook in blockchain technology- architecture, applications and challenges. *Int J Eng Res Technol* 12(12):2133–2137
12. Garg P, Gupta B, Chauhan AK, Sivarajah U, Gupta S, Modgil S (2021) Measuring the perceived benefits of implementing blockchain technology in the banking sector. In: *Technological forecasting and social change*, vol 163. <https://doi.org/10.1016/j.techfore.2020.120407>
13. Thakore R, Vaghashiya R, Patel C, Doshi N (2019) Blockchain - based IoT: a survey. In: *Procedia computer science*, vol 155, pp 704–709. Elsevier BV. <https://doi.org/10.1016/j.procs.2019.08.101>
14. State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time (2021) In: *IoT analytics*. <https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/>. Accessed 29 Jun 2021
15. Sarbabidya S, Saha T (2020) Role of chatbot in customer service: a study from the perspectives of the banking industry of Bangladesh. In: *International review of business research papers*, vol 16
16. Małek A. (2020) Internet of Things (IoT): considerations for life insurers. In: Borda M, Grima S, Kwiecień I (eds) *Life insurance in Europe. Financial and monetary policy studies*, vol 50. Springer, Cham. https://doi.org/10.1007/978-3-030-49655-5_1
17. Nakamoto S (2009) Bitcoin: a peer-to-peer electronic cash system. Retrieved from www.bitcoin.org
18. Peters GW, Panayi E (2015) Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money. Retrieved from <http://arxiv.org/abs/1511.05740>
19. Kumar A, Mahindru T, Shukla P, Sharan A (2020) Blockchain: the Indian strategy. Retrieved from: niti.gov.in. Accessed 7 April 21
20. Kitto Manda V (2018) Status check on blockchain implementations in India. Retrieved from <https://ssrn.com/abstract=3265654>
21. Karanjia B, Lakshman S, Goswami S (2017) Blockchain technology in India opportunities and challenges. Retrieved from: <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/strategy/in-strategy-innovation-blockchain-technology-india-opportunities-challenges-noexp.pdf>. Accessed 7 April 21
22. ICICI Bank Limited ICICI Bank Towers Bandra-Kurla Complex Bandra (E) Mumbai-400051. (2016). Retrieved from www.icicibank.com. Mutzel S (2021) Unlocking the payment experience: future imaginaries in the case of digital payments. *New Media Soc Sage*, 23(2):281–301
23. Lee I, Shin YJ (2018) Fintech: ecosystem, business models, investment decisions, and challenges. *Bus Horiz* 61(1):35–46. <https://doi.org/10.1016/j.bushor.2017.09.003>
24. Reuters T (2017) KYC compliance: the rising challenge for financial institutions. <https://d3kex6ty6anzzh.cloudfront.net/uploads/39/3973a2f5f7888855106b5d244df6192d0750c803.pdf>
25. Abelson H, Lessig L, Covell P, Gordon S, Hochberger A, Kovacs J, Schneck M (1998) Digital identity in cyberspace
26. Lang J (2017) Three uses for blockchain in banking. <http://www.ibm.com/blogs/blockchain/2017/10/three-uses-for-blockchain-in-banking/>
27. Polge J, Robert J, le Traon Y (2020) Permissioned blockchain frameworks in the industry: a comparison. *ICT Express*. <https://doi.org/10.1016/j.icte.2020.09.002>
28. Kapsoulis N, Psychas A, Palaiokrassas G, Marinakis A, Litke A, Varvarigou T (2020). Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture. *Future Internet* 12(2). <https://doi.org/10.3390/fi12020041>
29. Loader D (2019) Clearing, settlement and custody. Retrieved from www.securities-institute.org.uk

30. Miraz MH, Ali M, Excell PS, Picking R (2018) Internet of nano-things, things and everything: future growth trends. MDPI AG, Future Internet. <https://doi.org/10.3390/fi10080068>
31. Scott SV, Zachariadis M (n.d.) The society for worldwide interbank financial telecommunication (SWIFT): cooperative governance for network innovation, standards, and community
32. Reserve Bank of India Annual Report 2018-19 (2019). <https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs>
33. Bruno P, Denecker O, Niederkorn M (2019) Global payments report 2019: amid sustained growth, accelerating challenges demand bold actions. McKinsey global banking practice
34. Diamond DW (1984) Financial intermediation and delegated monitoring. Retrieved from <http://restud.oxfordjournals.org/>
35. Frame WS, White LJ, Berger AN, Molyneux P, Wilson JOS (2012) Technological change, financial innovation, and diffusion in banking prepared for the Oxford handbook of banking, 2nd edn
36. Guo Y, Liang C (2016) Blockchain application and outlook in the banking industry. SpringerOpen, financial innovation. <https://doi.org/10.1186/s40854-016-0034-9>
37. Crosby M, Pattanayak P, Verma S, Kalyanaraman V (2016) BlockChain technology: beyond bitcoin
38. Osmani M, El-Haddadeh R, Hindi N, Janssen M, Weerakkody V (2021) Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis. J Enterp Inf Manag 34(3):884–899. https://doi.org/10.1108/JEIM_02_2020_0044
39. Kim HM, Turesson H, Laskowski M, Bahreini AF, Permissionless and permissioned, technology-focused and business needs-driven: understanding the hybrid opportunity in blockchain through a case study of insolar. In: IEEE transactions on engineering management. <https://doi.org/10.1109/TEM.2020.3003565>

Identity Management in Internet of Things with Blockchain



Maria Polychronaki , Dimitrios G. Kogias ,
and Charalampos Z. Patrikakis

Abstract Internet of Things (IoT) is characterized by heterogeneity of devices, software and communication protocols when it comes to the implementation of any practical solutions. Especially in use cases such as smart cities, where scalability is very important and increased, the complexity of an Internet of Things system introduces issues on the management and privacy of both (smart) devices and users. Identity and access management is the set of policies applied on a system restricting or allowing access of acting entities (devices and users) to the system's services. OAuth and Single-Sign on are two of the widest used implementations for identity and access management. This book chapter targets exploring the new ways in which blockchain technology can significantly improve identity management in IoT by utilizing decentralized identity structures and specific cryptographic techniques applied by it.

Keywords Identity management · Decentralized identity · IAM · Blockchain · Cryptography

1 Introduction

Identity management is one of the most important key points when it comes to securing privacy in the Internet of Things. Devices need to communicate with each other, while at the same time humans are interacting with the system. The most unique aspect of IoT is that its purpose is not only to transfer data from one component to another but to make decisions based on those data. Considering the fact that these data

M. Polychronaki · D. G. Kogias · C. Z. Patrikakis

Department of Electrical and Electronics Engineering, University of West Attica, Attica, Greece
e-mail: m.polychronaki@uniwa.gr

D. G. Kogias
e-mail: dimikog@uniwa.gr

C. Z. Patrikakis
e-mail: bpatr@uniwa.gr

are, most of the time, sensitive and, therefore, must remain private identification and access management of the devices or services that request to read or process them is crucial to support the trust on the system and enhance its security and privacy characteristics.

In fact, there is a significant amount of research, backed up with real-world experiments, which agree on the importance of a robust identification system for IoT environments. For example, in [1–3], the authors come to the conclusion that applying a set of rules and using certain techniques for creating such a system strengthens the defense of the overall environment from threats like a phishing attack, sniffing attack, injections, data tampering, all kinds of unauthorized access from applications or users, Sybil Attacks and others. Because of these, the adaptation of the term *identity and access management (IAM)* was created, which led to various efforts to build IAM models to provide security and defense mechanisms for IoT over the last decade.

At the same time, blockchain technology has established itself beginning with the creation of Bitcoin [4], and then mainly via the decentralized finance (DeFi) sector where a significant amount of crypto-coins have been approved as fiat and can be used in various everyday economic transactions. Due to the revolution that blockchain has brought, both economically and technically, researchers are continuously trying to find different ways of combining it with other technologies. There is no doubt, as concluded in [5–7] among others, that while blockchain may introduce certain performance delays, the benefits which are introduced in IoT's identity management surpass those.

In this chapter, we will study the ways in which utilizing blockchain can benefit digital identity management in IoT systems. Specifically, we will discuss about models, architectures and algorithms for blockchain-enhanced IAM implementations for IoT, focusing on key features of blockchain which are ideal for the implementation of safe and completely private IAM systems, such as the Zero-Knowledge Proofs and Asymmetric Cryptography. In Sect. 1, the definition and the terminology of IAM and blockchain are presented along with the benefits of the blockchain's role in IAM processes. In Sect. 2, the basic concepts of IAM are introduced along with a presentation of the most known models on which modern IAM systems are relied on. In Sect. 3, the techniques that bring decentralization of IAM are thoroughly discussed, while in Sect. 4 the cryptographic tools of Zero-Knowledge Proofs (ZKP) and Decentralized Public Key Infrastructure (DPKI) are introduced along with practical examples and implementations that highlight the significant role they play in modern decentralized IAM applications. Last but not least, in Sect. 5 the significance, as well as the combination of the aforementioned tools, is concluded and the topics which need further research on decentralized IAM are briefly mentioned.

1.1 What is Identity Management

Generally, identity management is the idea of ensuring that specific people/users can (or cannot) access certain resources or places within an organization or closed environment. It is known with many abbreviations including IAM/IDAM/IDM (identity and access management), IGA (identity governance and administration), UM (user management), and AM (access management). From here on and through the rest of this chapter, identity management will be referred to as IAM.

In addition, in computer science, IAM is also known as a set of policies implemented using programming tools and techniques for managing and validating an entity's proper and, technically, legal access to data, services and applications [8]. This is a process that secures the interaction of applications with users and other applications or services as well and it works both ways. The system itself can be protected by some malicious activity by identifying who is trying to access its resources and making sure that they are who they say they are while, on the other hand, end users feel safe about their data privacy. Moreover, IAM can be used properly in order to give the functionality of control over one's data and who they can share it with.

1.2 Related Concepts and Terminology—IAM

Within the IoT context, an *identity* is the digital representation of any participant within a specific environment or domain (Fig. 1). The participants may be any person

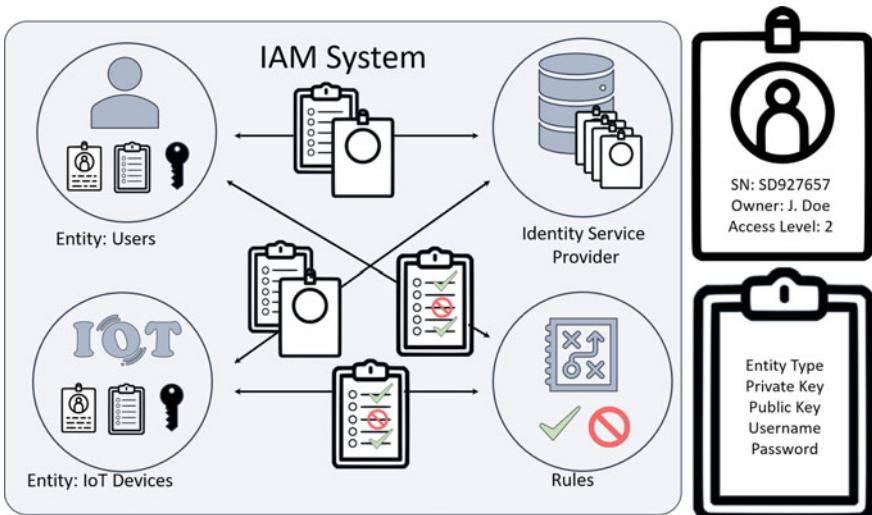


Fig. 1 (Left) Components and functionality of an IAM system (Right) Identity and attributes data example

or life form, any organization, any device or any entity which has a physical representation in the real world [9]. Thus, when the physical entity needs to interact with the IoT system, will do so via its own digital identity. This description of digital identity must not be misinterpreted with the very contemporary term of digital twin, which is a dynamic representation of a physical form. However, digital identities and specifically the decentralized identities can be a vital part of the authentication process of a digital twin in an IoT system, since the source of the data characterizing it must come from reliable sources.

Consequently, any entity which we want to be represented in the digital world should be characterized by a number of properties called *attributes*, such as a name, or a device serial number. These are to be used by the IAM system in order to establish different *roles* and their hierarchy within the IoT environment. Different roles may lead to different levels of access to data, services and applications (Fig. 1—Right).

Moreover, each identity must have a set of *credential* attributes in order to be validated and authenticated for, when the physical entity needs to interact with the system. For the IAM system to be able to distinguish between identities with similar or identical attributes, as many of those are dependent on the physical entity itself, every identity must have an *identifier* which will be unique for the corresponding environment that the IAM model is applied on.

Last but not least, the *identity provider* (IdP) is the system responsible for creating and managing these identities. Most of the time, IdP is another service running in the general service provider of an IoT system, which provides other services as well as telemetry or middleware communication.

Figure 1 illustrates these basic components of a traditional IAM system and the interaction between them. During the registration phase, the entities must communicate with the IdP to register themselves and make their presence known to the system by providing information regarding their attributes. After the registration is successfully completed, any time the respective entity needs to be authenticated and the corresponding application checks in with the authentication service in order to find out whether a particular entity is approved by the IAM rules to perform any actions.

1.3 Related Concepts and Terminology—Blockchain

Blockchain can be seen as a distributed network of unknown peers, which utilize strong cryptography techniques and consensus algorithms, in order to provide coordination and trust between untrusted participants. This definition concludes the philosophy of the blockchain-based IAM system, the participants of which do not trust each other and ask authentication and authorization from each other.

The *blockchain network* consists of a number of peers, which in the case of an IoT system could variate from any device with a minimum amount of processing power, to any server managed and built for the corresponding IoT system. The network's main purpose is to hold a distributed *ledger*, which contains blocks of data from

transactions in the network, each cryptographically chained with the next. The *peers* are responsible for running the necessary code and coming to a consensus regarding actions changing the ledger only through additions and never by deleting something that is already there.

Cryptographic techniques are vital for building trust between the unknown participants of the system [10]. Except for their use in binding the ledger blocks to form a chain, cryptographic tools and protocols are used in order to provide anonymity through private *keys*, which are held by every entity participating in the network. These keys provide anonymity as they are usually never combined with personal attributes, as well as the validity and authorization of any entity to interact with the network and change the ledger's state of data.

Lastly, *governance* is a concept rather new for the blockchain world but, ultimately, of extreme importance when it comes to building a hierarchy of trust and managing permissions and actions within an environment. Governance is used for applying rules and policies in decision-making within a closed environment where different actor roles exist.

1.4 The Benefits of Blockchain-Enhanced IAM

The current identity and access management mechanisms do succeed in providing the functionality needed for IoT identification of users and devices, however, the scalability of devices, services and applications are being cut off by the limitations of those mechanisms. A single IdP can only offer so much, while at the same time the centralization of IAM systems, working as centralized authorities, makes the whole IoT system vulnerable as they constitute a single point of failure (SPF). A more decentralized approach is less demanding in terms of performance for completing the tasks of IAM, while at the same time an identity can be validated and authenticated by any node from the blockchain network [11].

A blockchain-enhanced solution has the ability to natively remove any intermediaries (such as an IdP) or any service provider for that matter, whether it relates to IAM or not. Consequently, the interaction of users and devices, at least for authentication purposes can become more immediate and independent of a single service. It is worth noting that the removal of these services and their replacement with a blockchain network does not compromise security or privacy; on the contrary, it increases them by adding more cryptography algorithms and anonymity [12] (Fig. 2).

The immutability of the ledger can benefit the integrity of the logging process for the devices' interactions. Moreover, by giving the ownership of their identity to the users, they gain full control and management over their identity as well as the visibility of the data related to them. An example of such an implementation is the uPort short demonstration via the uPortlandia Demo [13]. In this demo, the user is called to download and use the uPort wallet application and go through the process of issuing a driver's license or a university diploma. Afterward, the user can choose to use one of the services offered in uPortlandia, but in order to do that they must

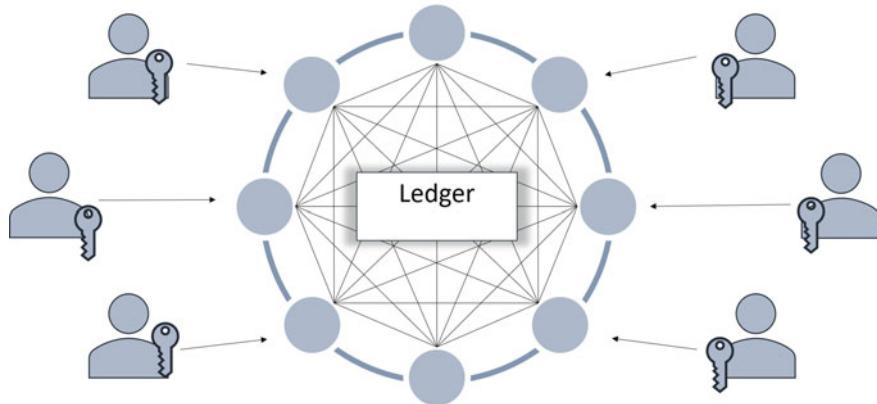


Fig. 2 The concept of decentralization in a blockchain system

authenticate themselves. This is achieved only via the user's wallet app, where their identity is stored, while the ledger only holds the validity of their driver's license or diploma.

Portability is also increased as every entity within the system will be holding their own identity as ownership. Any entity will be able to connect and be validated independently to multiple services and applications which do not need to be connected or correlated with each other but only be part of the same IoT ecosystem.

The benefits of using blockchain technology for IAM in IoT are significant for the advancement of IoT. This way, the creation of a decentralized identification layer is possible allowing different ecosystems to work together while users and devices have one uniform identity over the whole architecture.

2 Identity and Access Management (IAM)

IAM systems, apart from protecting a system from many security threats, are also applied for access control of resources. The creation of roles corresponding to specific permissions while forming a top-down restriction hierarchy is what defines the authentication levels regarding resource access. Applying rules regarding data accessibility for the acting entities in a system can significantly enhance user and system privacy. Thus, the creation of an IAM system must rely on a well-studied theoretical model for access management. In the following sections, the basic theoretical models on which the contemporary IAM systems are based will be presented as well as their basic responsibilities and principles.

2.1 Different IAM Models

There are two different IAM models which have increased popularity due to the ease of management they offer. These models are role-based access control (RBAC) and attribute-based access control (ABAC). While these are very general approaches and usually applied in environments regarding organizations and companies for managing access of stuff in data and local files, the resemblance of the administrative needs with an IoT environment is also apparent, since the only difference in the IoT environments is that of the existence of devices instead of users.

In more detail, RBAC (Fig. 3) uses a single-base model consisting of predefined *users*, *roles*, *permissions* and *sessions* to gradually build bottom-up models in order to add complexity and diversity to the model while defining the cardinality of roles [14]. Different users (or devices in the case of IoT) have different roles assigned to them, while permissions and sessions are granted as per those roles. Further tiers intend to introduce hierarchy and inheritance of permissions, as well as constraints within certain use case scenarios. The final model tier is used to combine the previous tiers and offer logic when some of the hierarchy and constraint rules are conflicted.

On the other hand, ABAC (Fig. 4) is a model designed to be built on attributes that characterize every entity within the corresponding environment. More specifically, ABAC considers users as *subjects* and resource entities as *objects* [15]. Both subjects and objects are characterized by a set of attributes, while at the same time there is a set of *access control rules* defined either before or after the initialization of the IAM system. When the corresponding environment conditions occur, the access control

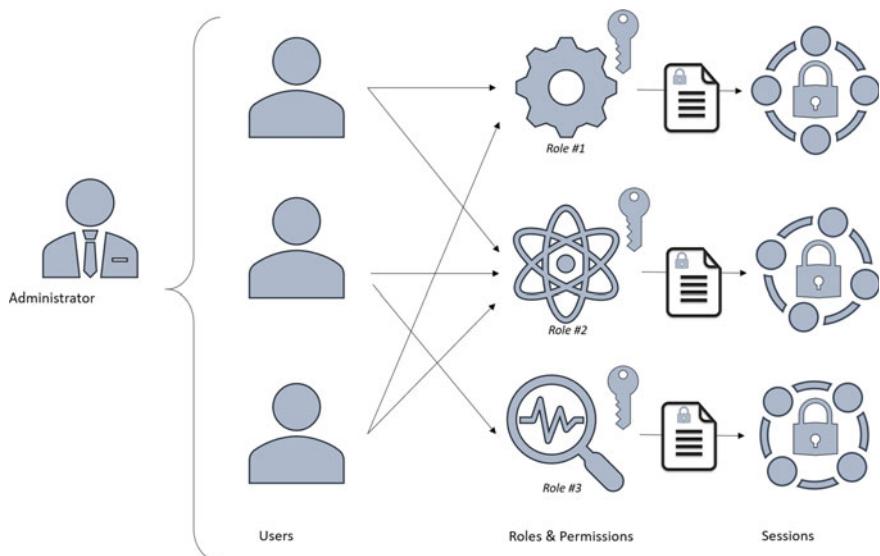


Fig. 3 Role based access control system

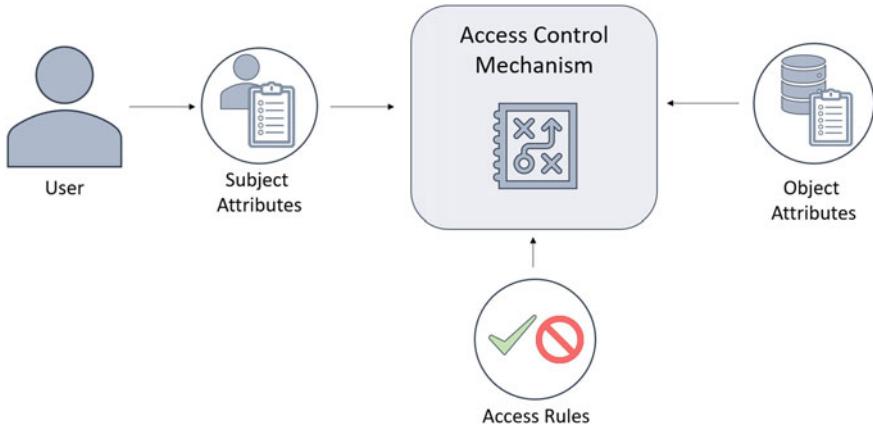


Fig. 4 Attribute-based access control system

rules are applied by the *access control mechanism (ACM)*. The ACM is essentially the point of the system where the decisions are made based on the policies configured by access control rules.

However, both of these models are designed to work under specific scenarios, thus producing disadvantages in some implementations [16]. For example, RBAC was designed for the case of only one administrator for IAM and problems arise when the administration is to be handled by multiple users. ABAC models heavily depend on the fine-grained design of the policy's architecture. This model cannot be efficiently applied when there are cross-interfering attributes for subjects causing errors in the access management functionality.

To solve the latter problem of the ABAC model, there have been efforts for designing further mechanisms for attribute quality management [16]. This means that subject and object attributes which are handled exclusively by the IAM system are contextually analyzed and evaluated for preventing logical failures due to conflicting attributes.

2.2 Responsibilities of IAM

The obligation of any IAM system is two-fold with the first to be identity management and the second is access management [8]. The first one is about all the processes which have an effect on the digital equivalent of an entity, which is its identity. Thus, identity management includes but is not limited to services for:

- Creation of an entity's identity
- Assignment of attributes to identities
- Management of login credentials

- Assigning and managing roles to identities
- Creation of groups of identities for mass management and scalability
- Applying policies of rules regarding all the above.

The second obligation of IAM is all about an entity's interaction with IoT and filtering which actions are allowed and which are not by the entity using its corresponding identity. Consequently, access management is used for:

- Allow or forbid access to services and resources
- Activity monitoring for administrative transparency
- Provisioning of data access for privacy
- Delegating access to private data or restricted services.

2.3 The Four Principles of Managing Identities and Access

By now it must be clear that IAM is not a specific framework or protocol which can be applied to a system and succeed in providing the services of the previous section, rather it is an abstract description of the functionalities it must offer. Every IoT environment has different needs, different kinds of entities that might interact with using a wide variety of communication protocols. This makes IAM a system whose architecture needs to be designed according to the respective IoT system's abstract architecture and functionality. So, in order to design a robust IAM architecture and choose the most suitable frameworks and protocols, one must consider the following features of IAM [17]:

- The Authentication Services: Authentication is the process with which an entity can verify itself using either something they know (e.g., password, seed phrase, mnemonic etc.), either something they own (e.g., tokens, certificate etc.) or something that characterizes them (e.g., biometric credentials, unique circuit characteristics etc.) [18].
- The Authorization Services: Authorization includes all the policies and rules which dictate what services and applications can be accessed by whom. Entities within a certain environment are assigned with roles and privileges that correspond to respective authorization levels, allowing them (or forbidding them) the access to resources.
- Identity Management: The identity management is the combination of technologies and tools for defining the digital identity for each entity, storing the identities' information and updating it when a change in an entity's account occurs. The revocation of a digital identity when necessary is also one of the tasks to be handled by the identity management services.
- Federated Identity (FId): When multiple applications or organizations must work within the same environment, while each of them has its own rules and policies, the use of a federated identity service can make things easier. Instead of the user providing credentials directly to each application, the FId acts as an intermediate

to all the applications on behalf of the user. Consequently, the user only needs to provide credentials to the FId, allowing him/her to use one account for multiple roles.

3 Decentralized Identity and Access Management

Decentralized identities are a core component of the decentralized identifiers standard (DID) [19]. Decentralization of IAM as a concept needs to be redesigned from scratch in order to provide an efficient, more secure solution. The DID standard, while it is not yet fully developed in order to be globally used, can provide the basis for creating architectures for decentralized IAM. In this section the basic components of a decentralized IAM will be presented, while their differences with the traditional centralized one will be mentioned.

3.1 New Concepts and Components

The centralized architecture models have a number of specific components. While their functionality remains the same in a decentralized model, the properties of these components must adapt accordingly.

In Table 1, the basic components of an IAM system are shown, as well as their counterparts in a decentralized architecture that is based on blockchain. These components can be divided into three major categories, network, logic and interface, according to their functionality within the IAM system.

3.1.1 Network: Identity Provider–Identity Issuer–Identity Validator

An identity provider is the component which facilitates the services, both for issuing a new identity or adding new attributes to existing identities and validating them. In a decentralized environment, these two functions can be separated and be distributed across the network running on different kinds of nodes, the *identity issuers* and the

Table 1 Centralized versus decentralized IAM components

	Centralized	Decentralized
Network	Identity provider	Identity issuer
		Identity validator
Logic	Authorization policies	Smart contracts
	Identity	Decentralized identity
Interface	User credentials	Personal wallet
	Login interface	

identity validators. Therefore, the single point of failure threat is removed, since client applications don't need to connect to the exact same service neither for *issuing* or modifying the identity nor for *validating* themselves when using resources.

3.1.2 Logic: Authorization Policies—Smart Contracts

Every IAM model is designed in order to keep hold of an environment-specific and hierarchic model, regarding who has the right to do what, or the logic of the IAM system. These, in a centralized system, are called policies and are implemented using an authorization framework (e.g., OAuth [20]). Blockchain can natively implement these policies using smart contracts, which are, essentially, code accessed by all the network nodes, or at least for those validating an entity. This way, the policies can be inspected by any node in the network while the validation process is open and can happen randomly throughout the network, eliminating the possibility of malevolently influencing one node to gain access.

3.1.3 Logic: Identity—Decentralized Identity

The identity component is the one holding the information of each entity in the system. All kinds of attributes that characterize each entity and its role in the system are contained to its identity. In the traditional centralized systems, entities (whether users or devices) do not hold their own identities. The identity provider holds all identities, and any entity asking access to a resource invokes their identity by providing their unique credentials (e.g., username, password).

A decentralized identity is a key component that revolutionizes the whole decentralized IAM architecture. It is comprised of the cryptographic information derived from the entity's unique properties, while it also contains its attributes. The main difference between the centralized identity and the decentralized one is that in the latter, each entity is the owner and the holder of their identity. Consequently, in that case, it must also be defined who can modify which attributes. An entity should have the right to modify some of the attributes of their identity (e.g., username), while some others (e.g., level of access) should be changed only by an identity issuer according to the rules specified in smart contracts. Another main difference is that since the identity is now stored locally and not at a central storage available to the whole network, then the attributes composing it can be aggregated by multiple issuers (technically multiple IdPs) [21]. In this context, a decentralized identity can also be the result of many issuing processes by many IdPs asserting multiple roles for the respective entity.

3.1.4 Interface: Credentials and Interface—Personal Wallet

In the centralized architecture, the invocation of an identity by an entity is succeeded using various methods. The most common one is providing the IdP with proof of knowledge. Proof of some information that only the specific entity would know or information that only the rightful owner of the particular identity should possess, like a set of username and password. Other methods are also used, but the basic interaction between the IdP and the entity remains the same, as the IdP remains the holder of all identities.

At the same time, in a decentralized architecture, the entities, being the holders of their DIDs, have the ability to control the visibility of certain parts of their identity, by invoking smart contract functions which allow the entities to alter the accessibility rules regarding exclusively their own data. There is no need for identity invocation, but only providing proof that their identity is valid, by communicating with any identity validator of the blockchain network.

In order to do that, each entity will need the proper software agent, which is able to contain the DID and provide the application interface (graphical user interface, programmable interface, etc.) for passing directly to the network the entity's desired modifications or asking for validation [22].

Blockchain is able to implement this software using Wallets, which are software used for safekeeping and handling the cryptographic keys of user accounts [23]. Wallets can be used and modified accordingly in order to keep and manage the DID of the entity. This way, the entity itself becomes the only owner of its identity and the visibility of its data is controlled exclusively by the entity.

Figure 5 illustrates how the basic components of a blockchain-based IAM system interact with each other. We can see that the blockchain comprised the identity validators and issuers who communicate over the blockchain network holding the common ledger. While it is mandatory for both of these components to be part of the blockchain network, it is not exclusive that only they must comprise it. Anyone who is willing to host a blockchain node and support the multiplication of the ledger can do so, without compromising any information due to the fact that the information on the ledger tends to be public. Users interact via their wallets which can directly communicate with the network over the internet and invoke smart contracts on behalf of the user's will.

3.2 The Self-sovereign Identity Model

For the last decade, the self-sovereign identity (SSI) [24] has been under the scope of many researchers because of the potential benefits it has to offer, not only in IoT but in any technological system which needs identity management to function properly. SSI, although not yet fully standardized regarding its implementation rules, it succeeds in putting the user right in the middle of the identity and access management system.

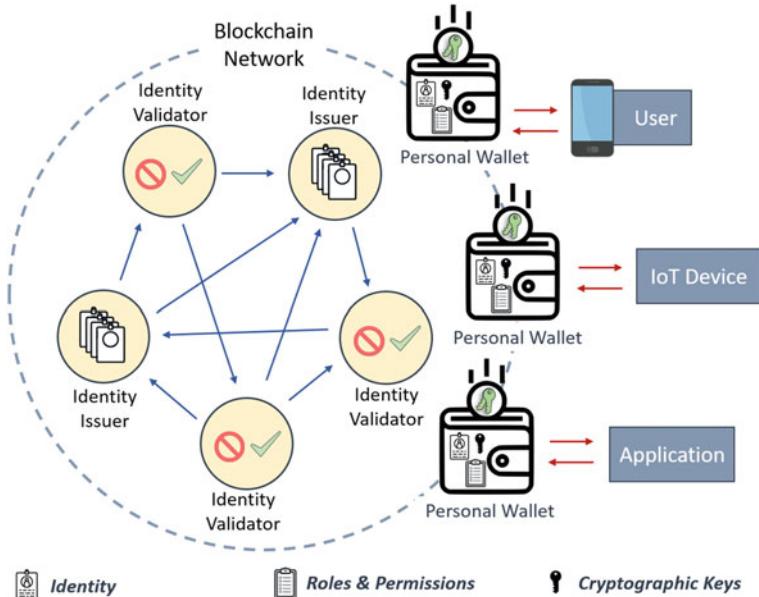


Fig. 5 Decentralized IAM

Allen [25] considers SSI to be the fourth and final stage of the identity evolution path. Centralized, federated and user-centric identities are the past three stages that fail to provide privacy and autonomy to the user. He attempts to define SSI using ten principles which ought to protect the user's control over their identity while the system maintains the proper transparency in order to obstruct any malevolent purpose.

These principles revolve around the rights of the user to being able to fully control, access and transfer their identity at will, while at the same time they have the right to consent (or not) to any kind of information sharing. The system for supporting SSI should provide algorithm transparency and persistence for the identities in order to be established and trusted throughout the network while the user can still claim their right-to-be-forgotten. Currently, there are two standards being developed by W3C to support the SSI implementation: The decentralized identifiers (DIDs) and the verifiable credentials (VCs) [26]. While the first one is more data-centric regarding the standardization information provided by W3C, the second one consisted of abstract concepts in order to give a fine-grained theoretical model of decentralized digital identities and the environments they should operate in.

3.2.1 Decentralized Identifiers (DIDs)

DIDs are based on the idea of globally unique identifiers. It is a new standard that allows entities to generate their own identities taking advantage of systems they trust, while they remain the true holders of their identities [19]. This standard focuses on the information which a decentralized identity should hold and on the description of the actors in a decentralized IAM architecture.

The DID standard is essentially a unique identifier comprising three sections:

- The “scheme DID” which is a specific JSON schema in order to provide context consistency
- The “DID method” which specifies the type of identity created and what methods are to be used on it (e.g., update, deactivate, etc.)
- The “Method specific identifier” which is the unique id number, resolving to a unique DID Document containing the entity’s attributes.

The DID document is the part of the identity which contains all the necessary information regarding the entity it represents. It may also contain the cryptographic material for verification on the system. Its attributes can be modified by the DID controller, the component with the capability to produce changes to the DID, if defined within the DID method.

Lastly, one more basic component is the verifiable data registry, which is the system running on top of a network, offering the necessary services for registering and returning data regarding DIDs. The most common examples of these are the distributed ledgers, such as blockchain, any decentralized file system or peer-to-peer network.

3.2.2 Verifiable Credentials (VCs)

On the other hand, VC is the standard which focuses on the cryptographic capabilities of an identity, aiming at the creation of digital credentials which are verifiable through the web, offering the same benefits with the physical ones (e.g., driver’s license) [26].

VCs are to be used with cryptographic technics and algorithms to produce different verifiable public keys for the properties an entity may want to proof, without compromising any personal details or information. This can be achieved by generating verifiable presentations, digitally signed by the entity in order to prove the ownership and authorship of the respective identity.

VCs are designed in such a way that they can provide privacy to the users as well as scalability to the system. Officially, the characteristics of this standard are specified within the scope of an ecosystem, which comprised three basic components, besides the holder of the identity:

- The Issuer: Issues VCs by checking with the verifiable data registry for valid identifiers and schemas to use
- The Validator: Responsible for validating the identifiers and schemas used through the verifiable data registry during the process of authorization or authentication
- The Verifiable Data Registry: The system which is able to create and validate identifiers, schemas, cryptographic keys or check the revocation list for a given identity. Trusted databases, decentralized databases and distributed ledgers are some of the examples of verifiable data registries.

The validity of a VC comes from the fact that it must contain certain information regarding the issuers and identifiers which is correlated with, as well as the cryptographic signatures which prove that the corresponding entity is the one unique holder of the identity.

3.3 SSI Implementations for IoT

IoT has proven to be one of the technologies that will shape the next-generation internet along with other technologies such as artificial intelligence and machine learning. However, the scalability of larger IoT ecosystems is constrained due to the performance issues which centralized architectures introduce, especially when it comes to preserving security and privacy. Blockchain can bring the decentralization of IoT and relieve the performance load allowing the ecosystems to scale both horizontally by multiplying the number of devices they can support and vertically by enhancing the functionality of each device, respectively.

In [27], the authors describe a framework for globally decentralized identity and access management for IoT (DIAM-IoT), which leverages the benefits which smart contracts and cryptographic wallets offer on a blockchain network. This framework focuses on the lack of device-specific functionalities which should be considered regarding the implementation of IAM systems for IoT. Thus, in the context of DIAM-IoT, it is supposed that IoT device manufacturers provided the blockchain network with their own specified smart contract in order to offer the end users the ability to register their own devices if they are willing to do so. DIAM-IoT utilizes both DIDs and VCs for binding devices with their owners using cryptographic keys and signed documents while through these the visibility over a device's data is also controlled with the permission of the owner.

The authors in [28], conducting a comparative analysis on different identity models and their implementation methods, presented the benefits of utilizing the SSI model in IoT contrasting existing solutions for identification such as X.509 certificates [29] or Pretty Good Privacy (PGP) [30]. Similarly, with the DIAM-IoT framework, the implementation of SSI is possible through the use of DID which is a combination of DID documents and VCs, which introduces true privacy and layered authentication across the users and devices of an IoT ecosystem.

Last but not least, Sovrin’s SSI use for IoT [31] is worth mentioning due to the in-depth analysis and fine-grained design of a decentralized IAM architecture, focusing on machine-to-machine (M2M) communication. The architecture is designed as such in order to handle the processor constraints of IoT devices’ performance. The lifecycle of devices consisted of two phases is presented while, once again, the use of DIDs and VCs is imperative in order to maintain privacy and control the access of devices and users to data without providing any piece of their identity content.

3.4 *The State of the SSI*

The SSI model has been implemented by various platforms, one of the most known is the Hyperledger Indy framework [32]. Sovrin along with Hyperledger build this framework which operates on a blockchain network and allows the creation of decentralized identities which are rooted on the blockchain but owned and managed by the users. Indy can also utilize cryptography libraries to enable Zero Knowledge Proofs (ZKPs) if the programmer chooses so. Unfortunately, Indy is not specified for use in IoT environments or devices, so its analysis was out of the scope of this paper. The wallet for interacting with the network is an application that must be programmed from zero while the computations which a Hyperledger Indy Node must perform cannot be supported by low-end devices.

On the other hand, there are several solutions of blockchain designed for IoT environments but they do not fully implement a truly decentralized identity model, rather they use gateways for the edge devices which are either communicating with the blockchain network or constitute a network node. IOTA [33] is a DLT platform and not blockchain, which is built considering the low computational power of IoT devices. Indeed, it allows for wallets to be used from low-end devices as well as be part of a network with the operation of a light node. However, IOTA up until very recently could not support smart contracts, making it impossible to implement any customized logic beyond simply inserting data in the ledger. Consequently, there was no way of implementing an IAM model using this network.

4 Cryptography: The Key to Privacy and Security

Throughout this chapter, the significance of cryptography is strongly pointed out several times. Truly, the basis of blockchain’s security is the use of cryptographic methods. Typically, there are two types of cryptography algorithms used in a blockchain network:

- Hashing algorithms for ensuring the property of the ledger’s chain, binding the blocks with each other, and for building a Merkle tree of all transactions written in the ledger.

- Asymmetric cryptography (also known as public–private key cryptography), which is applied roughly for giving the end users an identity in the network, and most importantly, for signing transactions upon the invocation of a smart contract.

The hashing algorithms ensure the immutability of the ledger via the creation of the Merkle tree, consistency to the network and enhanced security [34]. The consensus algorithm Proof-of-Work (PoW) is based on a hashing process that must result in a hash with specific characteristics (e.g., the first 5 digits should be zero). Hashing is mostly used in internal operations within the network.

The second type of cryptography is extremely important to be used properly from the corresponding wallet interacting with the network, especially considering the implementation of a decentralized IAM system. Wallets are the only known programmable tool capable of providing ownership of identity in a blockchain system, acting as the interface between the entities and the ledger. The authors of [34] having also analyzed the different types of attacks which can happen in a blockchain network show that there are at least three attacks that can compromise the identity of a user, not only by exposing their personal data but also by endangering the integrity of the network as well.

In the context of IoT, the use of cryptographic mechanisms must be reconsidered due to the fact that IoT devices have limited processing power, most of which will be used for their primary functions (e.g., measuring data from the physical world or having a mechanical part which must change state). The implementation of blockchain-centric cryptography methods in an IoT system is yet at its early stages. Over the next sections of this chapter, a short presentation of Zero-Knowledge Proofs (ZKPs) and Decentralized Public Key Infrastructure (DPKI) will take place from a blockchain perspective. ZKPs utilizing hashing algorithms and being performed off the blockchain network can provide anonymity to the authorization process, providing proofs instead of identity information. On the other hand, integrating DPKI offers all the advantages of the traditional PKI technology but in a decentralized manner.

4.1 Zero-Knowledge Proofs (ZKP)

Zero-Knowledge Proofs (ZKPs) have revolutionized modern cryptography and they can significantly upgrade blockchain technologies if used properly. ZKPs have emerged based on mathematical theorems and they constitute a large part of proof systems theory, where knowledge as a concept is statistically measured [35].

Zero-Knowledge systems function in an environment where a prover must convince a verifier about the validity of a statement, without revealing any additional information besides the statement itself. The verifier must probabilistically come to a conclusion where (s)he is convinced that the prover's statement is honest.

A Zero-Knowledge statement is to satisfy three explicit principles:



Fig. 6 The DID standard

- Completeness. An honest verifier should be convinced by the prover if the statement is true.
- Soundness. An honest verifier should NOT be convinced by the prover if the statement is false.
- Zero-Knowledge. The verifier has not acquired any further information besides the fact that the statement is true.

4.1.1 Interactive ZKPs

In order for the verifier to be convinced, a series of interactions between them and the prover must be conducted. The interaction process is randomized and the verifier tries to determine whether the prover's statement is true or not. A very simple example of an interactive ZKP method is that a prover states that he/she knows the answer to a sudoku puzzle but does not want to give away the answer to prove it.

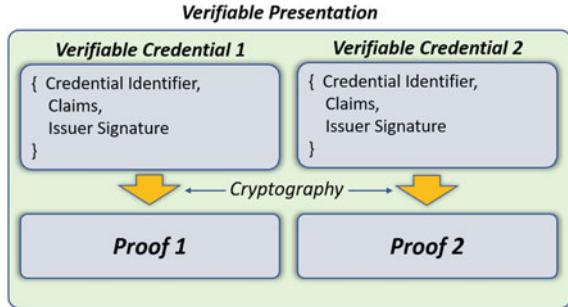
The verifier, in order to determine if this statement is true, asks the prover a series of questions to check the validity of the statement. One question could be to ask the prover "what is the position of numbers that fill a specific 3×3 box in a certain Sudoku puzzle". Another question the verifier could use is "How long could it take for an experienced user to solve a sudoku puzzle of given difficulty". Figure 6 shows the abstract interaction between the verifier and the prover in order to be persuaded about the latter's honesty.

The correct answer to these questions could persuade the verifier that the statement of the prover is valid, while the wrong answers could mean that the prover could not have solved a sudoku puzzle. The more of these questions are answered the higher the probability of the prover's honesty. At the same time, in order to avoid the scenario where the prover and the verifier have preconfigured the questions and answers, the randomization of these questions should be able to convince a third party for the statements validity as well (Figs. 7 and 8).

4.1.2 Non-interactive ZKPs

In non-interactive ZKP systems, the prover must shape an argument regarding the corresponding statement, which anyone can verify its validity. It is to be noted that non-interactive Zero-Knowledge is a mono-directional process where the prover

Fig. 7 The verifiable credentials standard logic



sends one and only one statement to the verifier [36]. While non-interactive ZKPs demand cryptography and number theory analysis in order to be fully explained, there is a simple example that is able to demonstrate their basic functionality.

Let's suppose that the prover and the verifier are two mathematicians (A and B, respectively) which know each other pretty well enjoying discussions related to math. They agreed on a common secret key for their communication. Now let's suppose that Mathematician A (Prover) wants to travel around the world while at the same time he develops a mathematical theorem (Fig. 9).

He wants to tell the Mathematician B (Verifier) and convince him that he has found the solution to his theorem but does not want to reveal the theorem nor its solution over mail. Moreover, because Mathematician A is traveling around the world, he does not have a stable address in order to be able to receive a mail back from his friend, meaning that their communication is one-way. How will Mathematician B be sure that this mail came from his friend and that he is telling the truth?

Mathematician A will use the secret key which they had previously agreed upon, in order to prove to his friend that it is him that is sending the mail, while at the same time he is telling the truth. The secret key could for example be a mathematical function with two parameters. In the mail, different parameters could be used every time but the correct pair and order of the parameters which satisfy their secret function can persuade Mathematician B whether it is his friend that the mail came from or not.

Figure 7 illustrates the one-way interaction between the prover and verifier, while their thoughts reveal the purpose of the non-interactive ZKPs usage.

4.1.3 ZKP Identity Adoptions in Blockchain

ZKPs are used in many ways in blockchain and not only for IAM. The very well-known Proof-of-Work (PoW) consensus used by the Bitcoin blockchain and the Ethereum blockchain platforms is based on the ZKP logic, with the proof being a single hash word which satisfies some requirements (among others, starting with an agreed by all peers, number of zeros). Thus, while there is no back-and-forth communication between the blockchain network nodes, all peers can verify whether

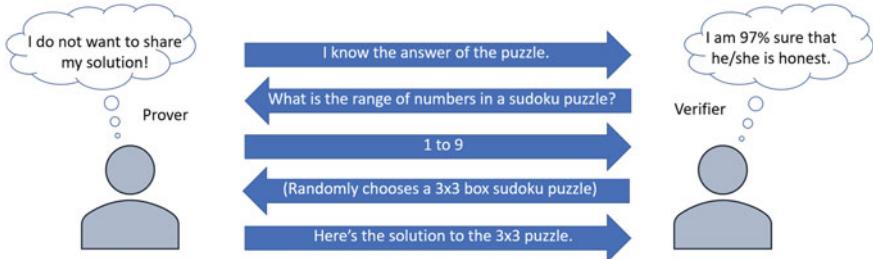


Fig. 8 Interactive ZKP proof process

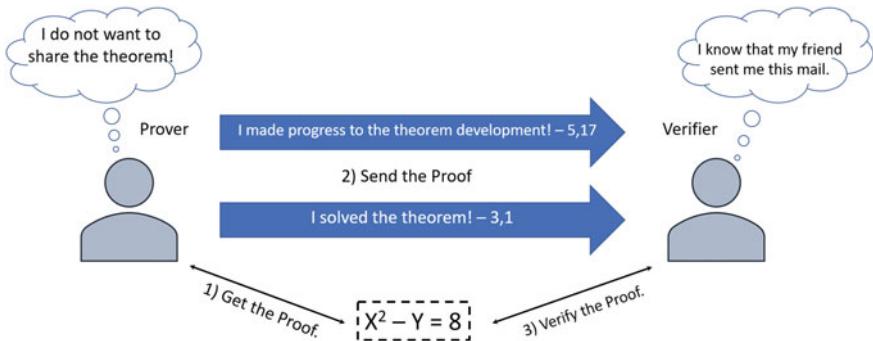


Fig. 9 Non-interactive ZKP process

a new block broadcasted is valid to be added onto the chain, while at the same time it acts as the proof that the node is willing to spend the computational power needed for the particular hash, thus making him an honest node to the network.

Another use of ZKP in blockchain is one of the Zerocoin protocols used by the Zerocoin blockchain. The authors in [37] present a solution for solving the privacy problem of Bitcoin, which has the weakness of back tracing a user's account using his/her transactions throughout the network. Zerocoin protocol breaks the links between transactions in a decentralized way, where users take advantage of an e-cash system to cryptographically mingle their coins with each other. Every user of Zerocoin becomes the miner of the Zerocoin coins equal to his/her bitcoin amount to be spent. Then, the specific amount of Bitcoin is locked, while the Zerocoin coins are bound with a public non-interactive ZKP, proving that someone knows to whom these coins came from (but not their name) and that he/she has the key which unlocks the corresponding Bitcoins. Any user who can validate this particular ZKP can exchange their Bitcoins with others, which previously were used by another user.

The Zcash blockchain performs transactions using a ZK-SNARKs protocol in order to hide the sensitive information contained in the transactions' data. Similarly, with Zerocoin, Zcash also targets the traceability of accounts in Bitcoin but from a different perspective. Instead of mingling users' coins, Zcash shields transactions

by not revealing the accounts involved in them using ZK-SNARKs proofs. The transactions are performed just like in the Bitcoin blockchain with the only difference that instead of logging accounts for the sender and the receiver of Bitcoins, the respective ZKP proofs are logged in the blocks. These proofs intent to persuade verifiers that the input and the output values sums are equal in UTXOs, the sender of a Bitcoin amount owns the private spending keys and that the transaction cannot be modified by anyone but those who participate in it [38].

4.1.4 ZKP Identity and Authentication Adoptions in IoT

The implementation of ZKPs in IoT is a matter rather difficult to be handled due to the low computational performance of low-end / edge devices such as sensors or actuators. Cryptographic computations are not simple and demand a small amount of core processing speed, which could be proved to be too high for such a device. This is why many of the solutions and algorithms which implicate ZKP and IoT for privacy and identification focus on the low computational need of generating a ZKP. Table 2 summarizes four ZKP-based solutions which have been tested in IoT environments and will be analyzed in this section.

The ZK-SNARKs can offer the potential of low computational need due to their “succinct” characteristic. In [39], the authors propose an architecture that utilizes ZK-SNARKs for producing VCs. However, their solution focuses on the network provenance of an IoT system and not on the authentication of low-end devices, while the performance tests are run using the Ethereum platform and a personal computer with considerably higher processing power.

In [40], a novel protocol named Zero-Knowledge Proof of Location (zk-Pol) is presented. Proof-of-Location is a technique where a user must provide a proof that he/she is located on a specific geographical area which is correlated to certain access points. The zk-Pol protocol offers security for IoT by leveraging the same technique and additionally maintains privacy by withholding the information of location using ZKPs. However, once again this protocol is focused on the users of an IoT system and not the edge devices, although the metrics of the experimental performance are rather efficient.

Finally, there is one type of ZKPs which is more suitable for IoT systems. They are called graph-based ZKP methods and their computations involve graph theory

Table 2 Brief comparison of ZKP protocols for IoT authentication

	Computational need	Data overhead	Point of application
ZK-Snarks	Low	Medium	Gateways
zk-Pol	Medium	Medium	Users’ interface
M-ZKP	Low	High	Edge
M-ZAS	Low	Low	Edge

mathematics. Regarding this type of proofs, the authors of [41] present the Multi-Graph Zero-Knowledge-based Authentication System (M-ZAS). It is composed of a two-procedure process, one of which is the Multi-Graph Zero-Knowledge Proof (M-ZKP). Typically, graph-based ZKPs are not demanding in terms of computational power but introduce high transmission overhead. However, the M-ZAS is designed in such a way reducing the overhead, making it a solution ideal for IoT edge devices.

Currently, to the best of our knowledge, the implementations of ZKP protocols using blockchain targeted for IoT devices authentication is a topic still under development and open for further research. Regardless, the philosophy of ZKP protocols has proven to be a flawless match for identification purposes [42] in decentralized IAM systems, where the environment is considered trustless.

4.2 Decentralized Public Key Infrastructure

Public key infrastructures (PKI) are revolutionary solutions regarding authentication [43]. Especially in IoT, most of the developed systems use one way or another PKI system, in order to authenticate devices using X.509 digital certificates [29]. This way, there is no need for using passwords, while at the same time devices are authenticated and the data exchanged are encrypted with these certificates. PKIs can provide the security and privacy needed for sensitive data transmission. Asymmetric encryption is the cryptographic process that takes place at the center of any PKI framework.

The PKI systems rely on a Certificate Authority (CA) which provides the certificates to devices and users. The communication over the internet is secured with the use of a cryptographic key pair (one public and one private) for encrypting and decrypting messages. At the same time, the proper use of these keys also provides the authentication of each user, since the decryption of messages relies on using the corresponding user's or device's public key. Traditionally, the PKI systems are based on centralized architectures, where the CA acts as a third party for multiple applications.

While PKI is the most frequently applied method of authentication, it has certain drawbacks. For starters, once again, the user is not the holder of his/her identity, rather only of the private key which authenticates him/her as the rightful owner of his/her identity held by the corresponding application's centralized IAM system. Moreover, with the CA relying on a centralized architecture, it can be targeted by cyber-criminals for man-in-the-middle (MITM) attacks. Lastly, of course, as with any centralized system, there is the danger of single point of failure (SPF), if for any reason the authorization service of a particular CA becomes unavailable.

PGP is one implementation of decentralized PKI (DPKI) which uses similar techniques as with X.509, but with the difference that we have a decentralized network where users can verify each other's signatures [44]. This architecture enables the "Web of Trust" where entities participating can decide whether they can trust one another based on previous and already trusted sources. When PGP was invented, blockchain technology was not yet developed, and this led to the failure of this

DKPI implementation due to issues regarding trusted third sources, since without blockchain there was no way of creating an environment of trust not between the CAs, nor between the users.

Blockchain solves the issue of trust due to the consensus algorithms obligating all peers to follow a protocol. This way, the ledger acts as a decentralized database and the peers of the blockchain as the third parties who do not trust each other forcing them to check the validity of one another. Solutions that are based on blockchain DPKIs for IoT are discussed below.

4.2.1 Blockchain DPKIs for IoT

The Ethereum network was the first public blockchain network which offered its users the ability to upload any smart contract they wanted using the specified programming language for it, solidity. Obviously, this paved the way for the redesign and further development of many systems and architectures which originally were based on a decentralized architecture.

The authors in [45] deploy and compare three different approaches for the authentication of IoT devices. One of the ways uses a blockchain type called Name/Value Storage (NVS), Emercoin, which binds IoT devices with unique tokens owned by the owners of the devices, while the other two approaches are based on the Ethereum network. The first demands from the IoT devices to communicate with a node of the Ethereum network, while the other incorporates a specific type of Ethereum node, called Light Sync Mode, within the IoT devices, allowing them to directly communicate and be part of the network.

All of these approaches rely on a device manager who is responsible for the registration process of every device. Additionally, the generation of the public keys is made possible via open-source programming libraries. The keys are used for creating the corresponding certificates for the devices, while they are also hashed along with a random serial number before they are logged in the Ethereum's ledger.

After comparing and contrasting these deployments, the authors concluded that in terms of speed the Emercoin implementation is the fastest since the process of authenticating is simplified using tokens. Either way, all the blockchain-based approaches are significantly faster than using a third trusted CA since the first takes at most 10 min while the second could take several hours or even days for issuing one certificate [45].

In terms of trust, it is incredibly important to notice that every blockchain-based implementation of a DPKI enforces the CAs to be authenticated with each other, hence removing the requirement of end users needing to trust a third party. However, this might not be the case in the implementation where the IoT devices are not directly communicating with the network and need a gateway to authenticate themselves.

Another interesting demonstration of NVS blockchain-based PKI focused on IoT devices is the one in [46]. The authors have designed the IoT-PKI architecture in great detail regarding the registration and authentication process of IoT devices using an NVS blockchain such as Emercoin or Namecoin. Similarly, as with the case in [45], the registration procedure needs a medium for communicating with the

blockchain network and a device setup process must take place before being able to be authenticated in the IoT system. More specifically, X.509 certificates are generated by the network nodes, while the private keys are generated directly in the IoT devices.

The implementation of this architecture led the authors to assess a use case of a DKPI in an IoT environment and concluded on a number of important security and functional failures, most of which can be handled if the respective measures are carefully taken during the implementation of the architecture.

Nonetheless, none of these solutions make use of the identity standards of DIDs or VCs, which means that their implementation process might prove to be rather time-consuming and will not be able to perform on a large-scale IoT ecosystem with multiple and heterogeneous IoT entities.

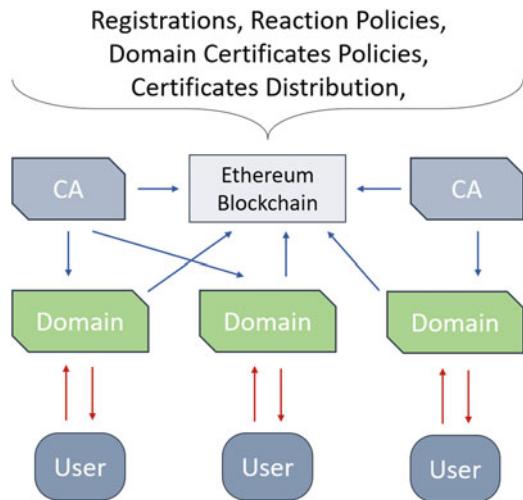
4.2.2 Instant Karma PKI (IKP)

The IKP [47] solution is a DPKI designed to work on the Ethereum blockchain and utilizes smart contracts in order to provide the functionality of its main entities. The scope of IKP is to build a network of CAs and domains used for the authorization and authentication of users. The registration process of a user is made by the domains which communicate with the CAs to get the certificates and interact with the ledger to log the registration. Smart contracts are used for every operation, as well as the registration of additional CAs or domains and broaden the IKP network.

The domains can negotiate with the CAs in order to agree upon a reaction policy contract function. These policies take action when unauthorized certificates are detected and act against any misbehavior by rewarding the peers who report these certificates. Another functionality of the IKP contract is to register to the ledger as per the Domain Certificate Policies, which define which CAs of each domain can communicate with in order to generate and register a new certificate (Fig. 10).

The IKP solution is based on the most popular smart contract-enabled blockchain network, the Ethereum while at the same time its design is rather fine-grained. This means that anyone can easily implement it using the guidelines of its creators. Despite this, it is not designed specifically for IoT environments, which possibly could result in implementation weaknesses or failures because of the extremely low computational performance of IoT devices. Moreover, we can see that IKP introduces a way for generating and distributing the certificates as well as authorizing and authenticating them using the blockchain network. However, it does not utilize either of the identity standards nor DIDs or VCs which have been developed for decentralized environments.

Fig. 10 Instant Karma PKI
(respectfully inspired from
[31])



5 Conclusions and Further Research

The previous sections presented the different aspects of blockchain-enhanced identity management for IoT, as shown in Table 3. The most abstract perspective of it is the IAM models which are designed from a more political point of view and specify not

Table 3 Summary of solutions presented in this chapter

		Implementations	Interpretation
IAM model (Self-sovereign identity)	Decentralized Identifiers (DIDs)	DIAM-IoT uPort IOTA	It is the digital component representing a physical/digital entity (e.g., person, device, service)
	Verifiable Credentials (VCs)	DIAM-IoT Hyperledger indy IOTA	Objects which anonymously prove an entity's property (e.g., Driver's License, ownership, IAM Role)
Cryptography	Zero Knowledge Proofs (ZKPs)	Zerocoins protocol ZK-SNARKs Zk-PoL M-ZKP M-SA2	Offers anonymity and privacy by generating cryptographic proofs (hashes) of information (e.g., Proof of having an IAM Role)
	Decentralized public key Infrastructure (DKPI)	Emercoin IoT—PKI IKP	Generating and Managing cryptographic certificates (or tokens) corresponding to the entities (e.g., X.509 certificates)

only how an entity can be identified in an IoT environment, but also the ways with which it can interact with other entities and the system itself providing data. The reason for which these models are so abstract is that IoT can be scaled and designed in many different ways, thus making the implementation of IAM a component that needs to be adapted depending on the IoT environment and architecture.

At the same time, digital identity is also evolving due to the significance of its use both in any IT implementation and in users' everyday life. Its uses find application in a wide spectrum of scenarios, from the simplest communication between a smartphone with a light bulb in a smart home, up to the identification of a digital twin in any environment. The SSI model is considered to be the last stage of the digital identity evolution, which can be owned and managed by entities themselves.

The combination of all the aforementioned technologies in this chapter is a matter yet open for further research and development. Performance in terms of speed as well as data consumption is a matter which needs to be carefully considered, especially for low-end devices operating on the edge. Many IoT systems are dependent on the time at the scale of milliseconds and at the same time cryptography (such as generating ZKPs) is rather costly in time and hardware in order to be fully implemented on the edge. A blockchain-enhanced IAM system adapted to IoT environments is to offer truly decentralized digital IAM, while every device and user is able to verify and be verified across an IoT network in real-time environments.

Considering of how much most, if not all, of the computer and information systems rely on the digital identity in order to provide authentication, authorization, as well as integrity and security, it is unquestionable that the decentralized identity is the future of a more secure and impenetrable identity management. Looking through the IoT point of view, decentralization is inevitable in order to offer scalability and distribute the data processing as well as the functionality throughout an IoT network. Blockchain, a decentralized technology that integrates cryptography all the way to its core functionalities, can lead the way onto a more decentralized and secure IoT especially when addressing the identity management issue.

References

1. Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W (2017) A survey on Internet of Things: architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things J* 4(5):1125–1142. <https://doi.org/10.1109/JIOT.2017.2683200>
2. Carmley P, Kettani H (2019) Identity and access management for the Internet of Things. *Int J Futur Comput Commun* 8(4):129–133
3. Vashi S, Ram J, Modi J, Verma S, Prakash C (2017) Internet of Things (IoT): a vision, architectural elements, and security issues. In: 2017 International conference on I-SMAC (IoT in social, mobile, analytics and cloud) (I-SMAC). Palladam, pp 492–496. <https://doi.org/10.1109/I-SMAC.2017.8058399>
4. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>
5. 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). Kona, HI, pp 618–623. <https://doi.org/10.1109/PERCOMW.2017.7917634>
- 6. Novo O (2018) Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J 5(2):1184–1195. <https://doi.org/10.1109/JIOT.2018.2812239>
 - 7. Huh S, Cho S, Kim S (2017) Managing IoT devices using blockchain platform. In: 2017 19th international conference on advanced communication technology (ICACT). Bongpyeong, pp 464–467. <https://doi.org/10.23919/ICACT.2017.7890132>
 - 8. Thakur MA, Gaikwad R (2015) User identity and access management trends in IT infrastructure- an overview. In: 2015 International conference on pervasive computing (ICPC). Pune, pp 1–4. <https://doi.org/10.1109/PERVASIVE.2015.7086972>
 - 9. Chen J, Liu Y, Chai Y (2015) An identity management framework for Internet of Things. In: 2015 IEEE 12th international conference on e-business engineering. Beijing, pp 360–364. <https://doi.org/10.1109/ICEBE.2015.67>
 - 10. Raikwar M, Gligoroski D, Kralevska K (2019) SoK of used cryptography in blockchain. IEEE Access 7:148550–148575. <https://doi.org/10.1109/ACCESS.2019.2946983>
 - 11. Kshetri N (2017) Can blockchain strengthen the Internet of Things? IT Prof 19(4):68–72. <https://doi.org/10.1109/MITP.2017.3051335>
 - 12. Rana R, Zaeem RN, Barber KS (2019) An assessment of blockchain identity solutions: minimizing risk and liability of authentication. In: 2019 IEEE/WIC/ACM international conference on web intelligence (WI). Thessaloniki, Greece, pp 26–33
 - 13. Consensys, (2019) Welcome to uPortlandia, the future of data and identity management, in medium. <https://media.consensys.net/welcome-to-uportlandia-the-future-of-data-and-identity-management-53220ea4e5c>. (Online)
 - 14. Sandhu RS, Coyne EJ, Feinstein HL, Youman CE (1996) Role-based access control models. Computer 29(2):38–47. <https://doi.org/10.1109/2.485845>
 - 15. Hu V, Kuhn VD, Ferraiolo D (2015) Attribute-based access control. Computer 48(2):85–88
 - 16. Kunz M, Puchta A, Groll S, Fuchs L, Pernul G (2019) Attribute quality management for dynamic identity and access management. J Inf Secur Appl 44:64–79
 - 17. Sharma A, Sharma S, Dave M (2015) Identity and access management- a comprehensive study. In: 2015 International conference on green computing and Internet of Things (ICGCIoT). Greater Noida, India, pp 1481–1485. <https://doi.org/10.1109/ICGCIoT.2015.7380701>
 - 18. Conrad E, Misenar S, Feldman J (2016) Domain 5: identity and access management (controlling access and managing identity). CISSP Study Guide 293–327
 - 19. W3 (2021), Decentralized Identifiers (DIDs) v1.0. W3.org. <https://www.w3.org/TR/did-core/>. (Online)
 - 20. Hardt D (2021) RFC 6749—the OAuth 2.0 authorization framework. Tools.ietf.org. <<https://tools.ietf.org/html/rfc6749>>. (Online)
 - 21. Grüner A, Mühle A, Gayvoronskaya T, Meinel C (2019) A comparative analysis of trust requirements in decentralized identity management. Adv Inf Netw Appl 200–213
 - 22. Dib O, Toumi K (2020) Decentralized identity systems: architecture, challenges, solutions and future directions. Ann Emerg Technol Comput 4(5):19–40. <https://doi.org/10.33166/aetic.2020.05.002>
 - 23. Kuperberg M (2020) Blockchain-based identity management: a survey from the enterprise and ecosystem perspective. IEEE Trans Eng Manage 67(4):1008–1027. <https://doi.org/10.1109/tem.2019.2926471>
 - 24. Toth KC, Anderson-Priddy A (2019) Self-sovereign digital identity: a paradigm shift for identity. IEEE Secur Priv 17(3):17–27. <https://doi.org/10.1109/MSEC.2018.2888782>
 - 25. Allen C, The path for self-sovereign identity. <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>
 - 26. W3 (2021) Verifiable credentials data model 1.0. W3.org. <https://www.w3.org/TR/vc-data-model/>. (Online)
 - 27. Fan X, Chai Q, Xu L, Guo D (2020) DIAM-IoT: a decentralized identity and access management framework for Internet of Things. In: Proceedings of the 2nd ACM international symposium on blockchain and secure critical infrastructure. <https://doi.org/10.1145/3384943.3409436>

28. Fedrecheski G, Rabaey JM, Costa LCP, Calcina Ccori PC, Pereira WT, Zuffo MK (2020) Self-sovereign identity for IoT environments: a perspective. In: 2020 global Internet of Things summit (GIoTS). Dublin, Ireland, pp 1–6. <https://doi.org/10.1109/GIOTS49054.2020.9119664>
29. Cooper D, Santesson S, Farrell S, Boeyen S, Housley R, Polk W (2008) Internet X.509 public key infrastructure certificate and certificate revocation List(CRL) profile. RFC Editor. <https://datatracker.ietf.org/doc/html/rfc5280>
30. Callas J, Donnerhacke L, Finney H, Shaw D, Thayer R (2007) RFC 4880—OpenPGP message format. Tools.ietf.org. <<https://tools.ietf.org/html/rfc4880>>. (Online)
31. Sovrin, Self-sovereign identity and IoT. In: Sovrin foundation SSI in IoT task force, 2020. <https://sovrin.org/library-iot>
32. Hyperledger. n.d. Hyperledger indy—hyperledger. <<https://www.hyperledger.org/use/hyperledger-indy>>. (Online)
33. Iota.org. n.d. <<https://www.iota.org/>>. (Online)
34. Dasgupta D, Shrein J, Gupta K (2019) A survey of blockchain from security perspective. J Bank Financ Technol 3(1):1–17. <https://doi.org/10.1007/s42786-018-00002-6>
35. Goldreich O (1993) A taxonomy of proof systems (part 1). SIGACT News 24:2–13. <https://doi.org/10.1145/164996.165000>
36. Blum M, Feldman P, Micali S (1988) Non-interactive zero-knowledge and its applications. In: Proceedings of the twentieth annual ACM symposium on Theory of computing—STOC '88. <https://doi.org/10.1145/62212.62222>
37. Miers I, Garman C, Green M, Rubin AD (2013) Zerocoins: anonymous distributed e-cash from bitcoin. In: 2013 IEEE symposium on security and privacy. Berkeley, CA, USA, pp 397–411. <https://doi.org/10.1109/SP.2013.34>
38. Petkus M (2019) Why and how zk-snark works. CoRR. [arXiv:abs/1906.07221](https://arxiv.org/abs/1906.07221). <http://arxiv.org/abs/1906.07221>. (Online)
39. Liu D, Ni J, Huang C, Lin X, Shen XS (2020) Secure and efficient distributed network provenance for IoT: a blockchain-based approach. IEEE Internet Things J 7(8):7564–7574. <https://doi.org/10.1109/JIOT.2020.2988481>
40. Wu W, Liu E, Gong X, Wang R (2020) Blockchain based zero-knowledge proof of location in IoT. In: ICC 2020—2020 IEEE international conference on communications (ICC). Dublin, Ireland, pp 1–7. <https://doi.org/10.1109/ICC40277.2020.9149366>
41. Chuang B, Guo J, Tsai J, Kuo Y (2017) Multi-graph Zero-knowledge-based authentication system in Internet of Things. In: 2017 IEEE international conference on communications (ICC). Paris, pp 1–6. <https://doi.org/10.1109/ICC.2017.7996820>
42. Springer, (2002) zero knowledge protocols. In: Fundamentals of cryptology. The international series in engineering and computer science, vol 528. Springer, Boston, MA. https://doi.org/10.1007/0-306-47053-5_14
43. Syngress, chapter 10—public key infrastructure. In: Dubrawsky I (ed) How to cheat, how to cheat at securing your network, syngress, 2007, pp 365–394. ISBN 9781597492317. <https://doi.org/10.1016/B978-159749231-7.50013-7>
44. Heinrich C Pretty good privacy (PGP). Encycl Cryptogr Secur 466–470. https://doi.org/10.1007/0-387-23483-7_310
45. Singla A, Bertino, E (2018) Blockchain-based PKI solutions for IoT. In: 2018 IEEE 4th international conference on collaboration and internet computing (CIC). Philadelphia, PA, USA, pp 9–15. <https://doi.org/10.1109/CIC.2018.00-45>
46. Won J, Singla A, Bertino E, Bollella G (2018) Decentralized public key infrastructure for Internet-of-Things. In: MILCOM 2018—2018 IEEE military communications conference (MILCOM). Los Angeles, CA, USA, pp 907–913. <https://doi.org/10.1109/MILCOM.2018.8599710>
47. Matsumoto S, Reischuk, RM (2017) IKP: turning a PKI around with decentralized automated incentives. In: 2017 IEEE symposium on security and privacy (SP). San Jose, CA, pp 410–426. <https://doi.org/10.1109/SP.2017.57>

An Efficient Hash-Selection-Based Blockchain Architecture for Industrial IoT (IIoT)



Susmit Das , Sreyashi Karmakar , and Himadri Nath Saha

Abstract Internet of Things is transforming devices making them “smart”, thereby overlapping the digital and physical worlds. Interaction between IoT devices creates networks with unprecedented scalability which, however, creates many exploitable vulnerabilities due to the lack of built-in security in IoT devices. Blockchain can resolve this particular limitation due to its immutable, decentralized nature. The industrial Internet of Things (IIoT) uses IoT devices to analyse and manage industrial data in real time for various purposes. Thus, protecting this data from different types of attacks is necessary, for which blockchain is viable. In this chapter, we have proposed a novel blockchain-based model that groups IIoT devices into tier-based clusters depending on computational capability by benchmarking. Each cluster is individually more efficient in terms of both energy utilization and security for IIoT systems by using different computationally suitable hash algorithms. The higher efficiency of our model compared to current solutions is proven by experimental results.

Keywords Blockchain · IIoT · IoT · Hash function · Security · Cryptography · Smart devices

1 Introduction

The Internet of Things (IoT) has nowadays become an important pillar of digital communication [1]. IoT is a network of interconnected electronic computing machines of various scales working in unison by exchange of information [2]. It is converting innumerable physical things into smart and responsive devices by extending their connectivity using the internet [3]. IoT is being employed in various

S. Das · S. Karmakar
RCC Institute of Information Technology, Kolkata, India

H. N. Saha ()
Surendranath Evening College, Calcutta University, Kolkata, India

industries for vast applications ranging from smart homes and cities to smart agriculture and healthcare amongst many others. Portable IoT sensory devices such as fitness trackers and IoT wearables are very common these days. Autonomous vehicles like self-driving cars take advantage of IoT to connect to the internet to share information from the sensors connected to cars to traffic sensors and sensors in parking areas. IoT devices typically have limited computational power, less storage space, but generate large amounts of data continuously. Recently, IoT is employed in the industrial sector to enhance the working system, like government and financial services, and so on to improve analysis and management systems [4]. These recent developments in IoT have led to the rise of the industrial Internet of Things (IIoT) which can completely change the landscape upon global adoption [5]. Though IoT provides rewarding benefits, the network faces various privacy and reliability risks [6]. Among the challenges, the security of the bulk amount of sensed IIoT data and privacy preservation are the most critical issues [7]. With IIoT implementations, there is a need to focus on the security of industrial data. Security remains an issue of high priority where many can stumble when integrating IIoT into their operations. In general, IIoT devices face risks to a great extent mainly because the devices lack the required security incorporated to counter the threats faced [8]. Along with the technical issues, users play a huge role in the vulnerability of these devices. Some notable reasons for the vulnerability of smart devices are [9]:

- The hardware and computational ability of IoT devices are fairly limited. As such, they are only able to perform the definite tasks permitted by the limited infrastructure.
- These tasks include handling sizable amounts of data from various sources. Unfortunately, the lack of inbuilt security measures leaves these data open to attacks.
- The nature of the devices and technologies used in IoT networks for the transmission of data is heterogeneous. Hence, it is unviable to maintain unified standard protocols or methods for the protection of the data [10].
- Apart from these, many of the devices used in IoT networks often have several individual vulnerabilities that compromise the security of the entire IoT ecosystem.
- The lack of general awareness for data security amongst users exposes the vulnerabilities to potential attackers.

The security loopholes make way for cybercrimes. These cracks become a cyber-criminals' foothold to launch various attacks. It is very vital to secure such crucial sensed data. The emergence of blockchain technology demonstrates encouraging possibilities to enhance the security of IoT systems. The immutable, decentralized and anonymous technology is transforming industries by enabling trustful transactions. Thus, it improves system security by decreasing system risks, reducing the severity of financial frauds, and diminishing operational costs. To overcome the

shortcomings of IIoT the convergence of IIoT and blockchain is a promising possibility [11]. Thus, expanding the revolutionary secure integration of IoT in industry. The most rewarding feature of blockchain is its decentralized, distributed nature which makes peer-to-peer transactions trustful. It enhances the overall security by time-stamping transactions along with the use of consensus algorithms and highly expensive encryption functions. External and overhead costs are minimized, the efficiency of the network is increased, and the problem of insecure data storage in centralized frameworks is solved [12].

2 Motivations

The primary motivations of our work are:

- Carrying out a background study on the viability of blockchain usage for securing data in IIoT applications.
- Performing a case study of existing blockchain models for IoT.
- Studying the constraints and limitations faced by implementations of blockchain in IIoT ecosystems.
- Developing a novel blockchain architecture that can achieve the highest possible efficiency by countering these limitations and can be used with a wide range of IIoT devices natively.
- Making sure the proposed model is crypto agile so that it can be appropriately updated with newer technologies in this field.
- Designing the necessary algorithms to provide software support for the blockchain architecture in a way that is universally compatible with any IIoT hardware.
- Implementing our novel architecture in a simulated IIoT environment.
- Evaluating the performance of this implementation and analysing the results to prove the efficiency of our model.

In the coming sections, the basics of blockchain and IoT are analysed, and then the main features of blockchain, such as decentralization, smart contracts, asymmetric encryption, and others that can be utilized on the IoT platform to promote its functions are explored. Hence, concluding that IIoT can be secured by the decentralized technology, blockchain.

The paper is divided as in Sect. 3, we will perform a background study of blockchain technology, various features pertaining to it, and possibilities of implementing blockchain in industrial IoT (IIoT) as well as perform a detailed literature review of issues faced by current developments in this area. In Sect. 4, we have proposed a model that focuses on the efficient application of blockchain in IIoT ecosystems and its methodology is discussed in Sect. 5. The implementation of this model is presented in Sect. 6. In Sect. 7, a comparative result analysis is prepared to test the model and its implementation. We have compared our proposed model to

the Bitcoin model to prove its efficiency in Sect. 8. In Sect. 9, the future research directions are mentioned and finally, Sect. 10 concludes the work and the references used are documented.

3 Background and Related Work

Blockchain is an auditable, immutable, time-stamped distributed ledger of blocks. It securely stores the details of every transaction performed in the network. The immutable ledger technology uses a peer-to-peer network in order to maintain security and anonymity [13]. Each participating node present in the blockchain network preserves a complete copy of the ledger. These ledgers update continuously, on the validation of each transaction [13]. Initially, blockchain was proposed for executing online exchanges using digital currency. The first proof-of-work blockchain system was Bitcoin's Genesis Block. It is the most appropriate for the cybersecurity ecosystem [14] due to its advantageous features like its decentralized, immutable nature suitable for peer-to-peer networks. It is the task of every node participating in the network to verify and validate every new transaction, thus eliminating security risks and the need for a central authority. Some special nodes present in the network are miners. They process and confirm transactions using specially designed computationally powerful computers. The miners [15] perform a very critical mathematical problem to solve the nonce and generate the proof-of-work, in return the miners are rewarded. This process adds the transaction records to the public ledger of past transactions. This way every data and transaction is cryptographically encoded and secured.

With the advancements in technology, the implementation of IoT is expanding in different industrial sectors like production, manufacturing and fabrication industries. This digital transformation of industry led to the fourth industrial revolution, i.e., Industry 4.0. It is introducing automation along with new ways of production with real-time optimization and remote monitoring. As these devices perform such crucial tasks, it is necessary to secure the critical data handled in the process. So, a new paradigm for secure data preservation has evolved; it is called blockchain. Blockchain technology, due to its secure nature, is the most suitable solution to safeguard the system from various kinds of attacks ranging from common denial-of-service-based attacks to elaborate cryptanalytic attacks. It has gained a lot of focus in the industry due to its inherent security qualities, like the application of principles of cryptography to ensure data immutability and security. Although there are many positive aspects of blockchain-enabled IIoT, there are some limitations that still persist. The opportunity cost of integrating blockchain with IoT in specific conditions can be very high due to certain limitations [16]. Much research work from multiple approaches is being conducted for ensuring a stable, secure blockchain-IIoT integration. It is an urgent need of the hour to solve the issues for an efficient inclusion of blockchain in IIoT.

Although there have been several works aiming to overcome the limitations of blockchain-enabled IIoT, an efficient blockchain solution for IIoT is still limited. To

overcome the challenges, present in IIoT, with the lightweight solution of blockchain technology, the research [15] proposed lightweight scalable blockchain (LSB), which was enhanced as needed for IoT. It provided end-to-end security where the first blockchain creation became decentralized by devising an overlay network. The entire network is arranged in discrete clusters that reduce overheads and look after and manage the blockchain. The mining process is very costly, so to reduce its processing overhead and delay, a distributed time-based consensus algorithm (DTC) is proposed. The LSB also includes an algorithm to ensure that the throughput of the blockchain does not deviate from the cumulative transaction load in the network. A lightweight consensus algorithm is proposed to build a trustworthy, distributed system. To optimize the blockchain, a throughput management algorithm is used. In [17] the authors have developed and proposed a lightweight method for merging IoT with blockchain called “LightChain”. The proposed method combines the available resources and solves the PoW puzzles, which is not feasible for individual devices. The results of the model clearly depict that even with the increase in the number of clusters, the model is able to effectively utilize the resources. Another blockchain system for IIoT called LightChain was proposed by the authors of different research work [18]. The model comprises a lightweight data structure termed LightBlock and a consensus algorithm with a synergistic multiple proof mechanism. The cooperation among the IIoT devices is provoked by the consensus mechanism. In [19] the authors proposed a model for the hyper ledger fabric, which is built on a Byzantine fault-tolerant consensus algorithm. This consensus algorithm is responsible for system throughput and transaction confirmation time. To show the application range of BlockChain, the researcher [20] has put forward an adaptable blockchain protocol called Proof-of-Property (PoP), which allows the devices to validate the incoming transactions without downloading the whole blockchain initially. In the research [21] the authors have proposed a blockchain design for IIoT with Lightweight Hash function and this hash can change flexibly, depending on transactions. It is the responsibility of the cell nodes to select the appropriate hash function along with the collection of the transactions from various field devices and control devices. In the research [22] the authors made a model named, Rapid Chain, which attempted to improve the broadcast latency and storage consumption by dividing the entire P2P network into smaller groups. The leadership selection and cross-chain mechanism in Bitcoin-NG and Multi-chain helped to improve blockchain scalability. There is another research [23], where blockchain architecture is designed using Lightweight Hash functions for IIoT. Here the hash changes depend on the number of transactions. The nodes collect the transactions from the field devices and control devices and select the appropriate hash functions as required. The research [24] introduced a signature theory with a ring-like structure. To let the nodes join or leave the network dynamically, the ElGamal digital signature algorithm and the PBFT algorithm improve the signature and verification process. The research [25] has proposed a new design of blockchain with an optimized hash algorithm based on the proactive reconfigurable computing architecture (PRCA) where the performance of the blockchain hash function is improved to ensure security and integrity, and for exchanging data and information, multiple lightweight hash algorithms are employed. The attack

surface is expanded and to improve the attack threshold the hardware is utilized. The research [26] proposed a lightweight blockchain called Sensor Chain, which is a large global blockchain divided into local blockchains. Sensor Chain requires much less storage space than a normal blockchain and optimizes blockchain with respect to memory space requirement and latency. A mechanism based on credit, and alliance chain-based credit evaluation was proposed named, practical Byzantine fault-tolerant (PBFT) consensus mechanism and a lightweight consistency protocol is utilized. A modified checkpoint protocol enables the nodes to dynamically enter or leave the system. In the research [27] the authors have proposed an algorithm, called the Ouroboros algorithm. This algorithm aims to prevent attacks caused by selfish mining by demonstrating the Nash equilibrium by the non-malicious nodes in the network. This is performed after a consensus algorithm that forms a Proof-of-Stake algorithm is generated by an incentive system. The other algorithm is a Proof-of-Work algorithm based on the famous “generalized birthday paradox” named the Equihash algorithm. It determines the workload by calculating the memory required from the sizes of the nodes since it is a memory-dependent algorithm. Though the algorithm demands a good amount of space it achieves immediate verification. It improves the cost-effectiveness of the ASCI hardware. A private immutable ledger, designed in the research [28] acts as a blockchain but is managed centrally. The devices with greater resources implement a publicly accessible distributed system.

From the above literature review, it is worth marking that lightweight blockchain has the potential to successfully merge IIoT technology with blockchain [29]. We conclude that some developments in lightweight blockchain architecture have been done. Some have built reinforcement learning in blockchain [30] to provide rapid adoption of blockchain technology. And others have designed a lightweight hash-based blockchain for resource-constrained devices to reduce the computational burden and block creation latency [31]. Existing systems also sometimes lack the potential to find an efficient and optimized blockchain design to secure the IIoT network. The motivation of the work is not only to design an efficient hash functioned blockchain but also optimally use the computing resources of IIoT devices.

However, even though lightweight cryptographic hash algorithms have a lot of potential use cases in IIoT, they all share some glaring issues like a significant lack of bandwidth, lack of software support as well as being generally more vulnerable compared to more robust cryptographic hash algorithms. Especially more computationally capable devices in the IIoT network, where high bandwidth is necessary, just using lightweight blockchain can be contra-productive to the efficiency of the network. As such, there is the need for a more efficient architecture that merges the advantages of both lightweight cryptography and non-lightweight cryptography to avoid a bandwidth bottleneck while also taking into account the computational powers of the devices in the IIoT network.

Also, one of the biggest questions over the use of blockchain in industrial usage is whether the security it provides is worth the opportunity cost and the jury is still out on its sufficiency in the event of a data breach. Blockchains ultimately depend on the cryptographic hash function that is used for security. However as strong as hash functions are, they are not impermeable. One common example is the downfall of SHA-1, whose once 159-bit protection got theoretically reduced to just 57.5 bits due to various collision attacks by 2012. By 2017, a lot of vendors migrated a significant portion of their customers to the newer SHA-2. On February 23, 2017, Google announced the first collision of SHA-1, marking the end of the SHA-1 era [32]. However, the process of migration from SHA-1 to SHA-2 was needlessly over-complicated due to the initial lack of developer support on both hardware and software ends. Even though SHA-2 is still considered secure, it uses a very similar base algorithm as SHA-1, making it a ticking time bomb before it gets cracked like its predecessor. But we are still facing the same dilemma with migration to SHA-3-based algorithms from SHA-2 due to the same issue of lack of hardware or software support. This leads to yet another hurdle of widespread adoption of blockchain, one that can be solved with a system in place to provide the much-needed crypto agility required for increased future-proofing. Cybersecurity is an ever-evolving landscape and as such, there is a need for an architecture that can make transitions in algorithms as seamless as possible. Lack of crypto agility felt like the final problem that needs to be solved in our search for efficiency.

Seamless integration between technologies of blockchain and IIoT will require lightweight cryptographic systems as well as their more robust counterparts working in sync. In this work, we explore an efficient method for this convergence by using cryptographic hash functions efficiently depending on the computational power of the devices. The main objective of the proposed model is to reduce the computational burden and block creation latency that the current blockchain suffers from and optimally use the computational resources based on the processor's power.

4 Proposed Model

A model is proposed that focuses on the adaptation of an architecture of blockchain that dynamically assigns efficient hash functions according to the required needs and available computational power to overcome some of the challenges of blockchain-IIoT integration. The blockchain field is an ever-growing area in which researchers are finding new possible ways to improve core blockchain technology itself. Blockchain decentralization property is mainly because of the hash function, the proper selection of this hash function is fundamental to the efficiency of the system. The challenge to implement these technologies is due to the resource-constrained nature of IIoT. Blockchain as a technology is still new from an industrial standpoint. While we can see blockchain being adopted over traditional databases in a number of industries, there are still some hurdles on its way to widespread industry adoption, especially for providing security in IoT-based applications over traditional centralized systems.

From a financial point of view, efficiency is the most universally important aspect of any technology for any industry. The efficiency of a blockchain in any system can differ significantly depending on the type of consensus algorithm and cryptographic hashing algorithm used as well as the computational power of the IIoT device in question. All cryptographic hashing functions have different complexity, levels of provided security and often have their own vulnerabilities.

The aim of the proposed model is to create a system that caters to a range of devices with varying computational powers, instead of going with the common route of trying to find “a size that fits all”. So, we have chosen a context-aware solution that dynamically adjusts to the specific needs of the device and the computation power available. To achieve this, a benchmarking algorithm is designed, which is used to estimate the computational power of various IoT devices in the network. This benchmarking algorithm consists of multiple trigonometric functions that are repeated over the entire 360° range and iterated multiple times in a fixed amount of time. While there are other functions like matrix manipulation functions and prime number generation functions that are used by some other benchmarking algorithms, these can overwhelm the weaker processors of some low-power IIoT devices resulting in inconsistencies. Trigonometric functions are very complex and the sheer number of calculations can stress the processors of a wider range of devices without any inconsistencies. As the time of operation is fixed, the number of iterations achieved within the fixed time gives a fair indication of the computational power of the processor used. Compared to other methods of processor benchmarking that can take hours on weaker hardware, this is a much more time-efficient process as the fixed time can be set to very low. The average number of iterations achieved is the output benchmark score.

The output score from the benchmarking function is used to generate a device-specific token, which is stored in the device for future reference. This token contains the benchmark score achieved by the device and is used to categorize the huge range of possible IIoT devices into multiple tiers. In our case, the devices are classified into four tiers, Tier I to IV, with ascending computational power, where Tier I consists of low-power devices and Tier IV consists of computationally high-power devices.

Now, the IoT network is split into numerous virtual clusters of IIoT devices, according to their tier. Every tier is accordingly assigned a unique hashing algorithm, which is most suited for the processing power of its devices and is most appropriate for the data it is storing. When the consensus algorithm is called, the token of the concerned device is checked to find its tier as shown in Fig. 1. Its respective hash function is used to generate the hash. As such, we have various parallel blockchains in place all with their unique hashing algorithm in the entire IoT network. This makes the overall system more secure as it is difficult for attackers to identify the hash algorithm being used, with the IoT network separated into different clusters of IIoT devices as demonstrated in Fig. 2. By having a system in place that can assign different hash functions, we also solve the problem of not having enough crypto agility partially, as this architecture allows any vendor to add or update their blockchain to any hash function as needed at least from the software side as long as

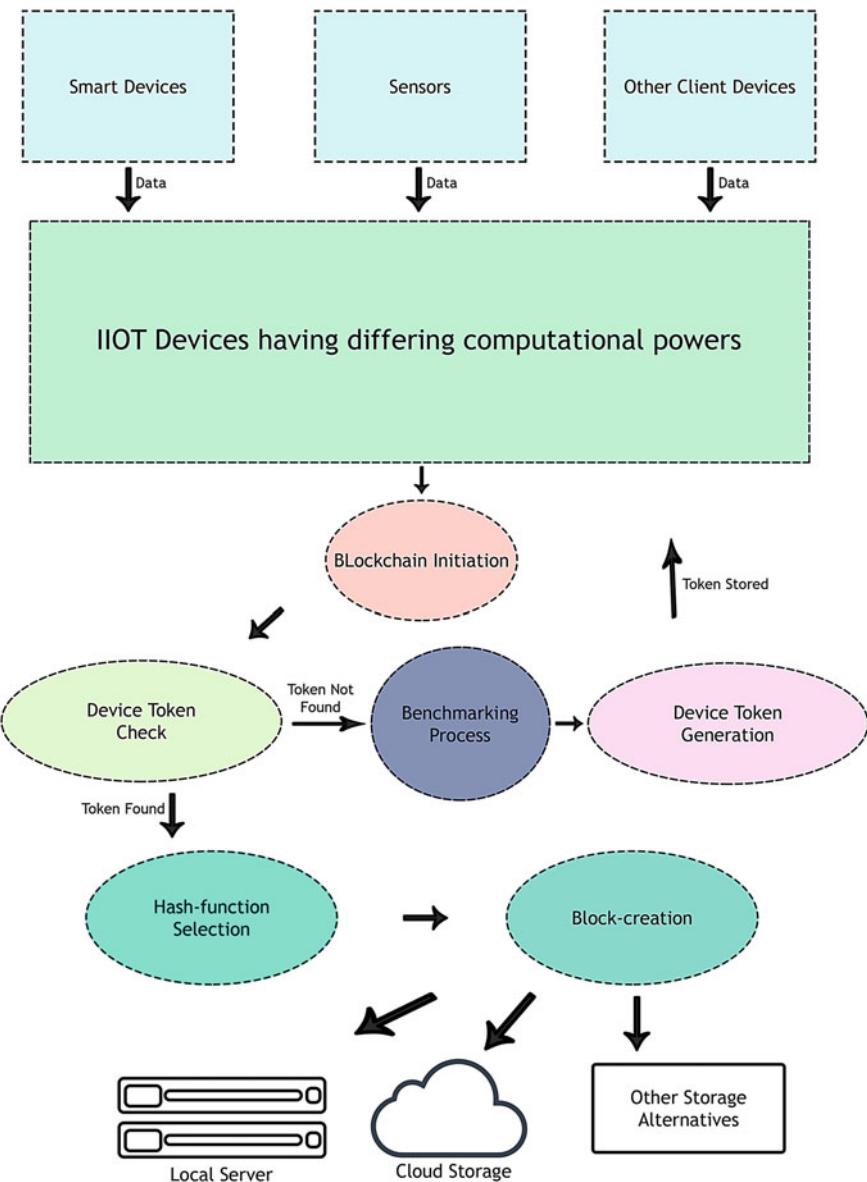


Fig. 1 Proposed model

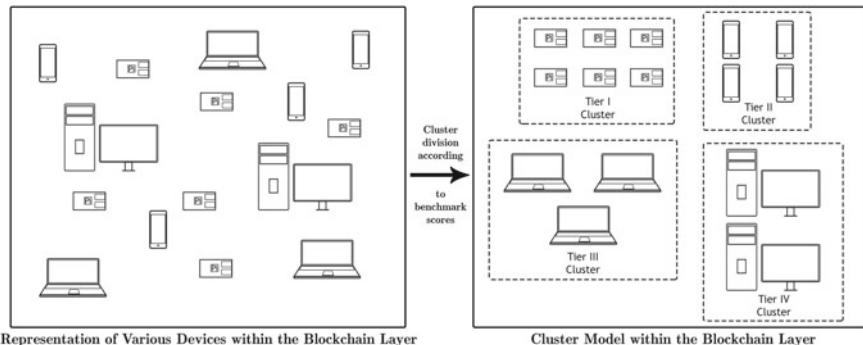


Fig. 2 Tier-based cluster of IIoT devices

hardware support exists for the platform, thus making the system future-proof and increases the financial efficiency of the system as well. By intelligently splitting all the computationally variable devices into clusters of similar computational power devices, we also avoid one potential issue of redundant mirroring of unnecessary blockchain data.

In an industrial environment, generally, there are several input streams of data like sensor data, device data, log data and many more into IIoT devices having different computation capabilities. On receiving the input, the IIoT devices initiate blockchain formation for storing these data. To check the tier type of the device, the token of that particular device is searched for. If the token already exists, an appropriate hash algorithm is selected. If it is a new device where the token has not been generated, the earlier benchmarking process is executed, generating the token and storing it in the device. Next, the appropriate hash algorithm is used for blockchain creation. Then the data is stored in a decentralized manner in local servers or in the cloud or any other storage devices. This mechanism is depicted in Fig. 1.

The vital part of this model is selecting appropriate hash algorithms. The hash function is the most important part of any cryptographic blockchain system and as such, it is a fundamental component of blockchain technology. Hashing is a method of applying the hash function to data to compute a relatively unique output for all inputs as in Fig. 3. The procedure is called message digest. It allows to independently acquire hash data from input data and produce the same results on applying the same input, proving that the data has not changed. Different hash algorithms have different properties, so all of them provides differing levels of security and can have different vulnerabilities. We take a look at some of these properties in Table 1.

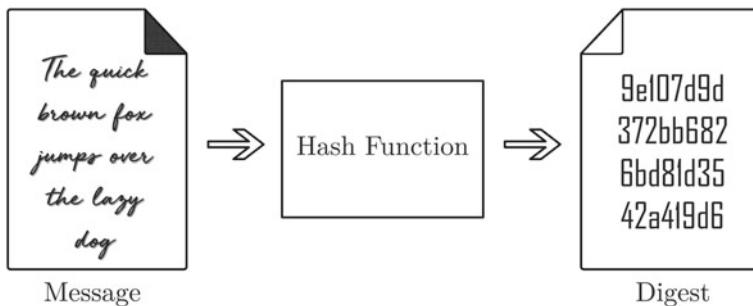


Fig. 3 Hashing an input message

There can be some rare applications in IIoT that strictly require the usage of a single hash algorithm throughout the entire system. In these cases, a slightly modified version of this model can be used. In the modified architecture, because different hash algorithms can't be assigned to the different tiers of devices, instead different target mathematical difficulties are assigned to different tiers of devices in the consensus algorithm with one single hash algorithm being used throughout the entire network.

This model is fully modular and efficient as well as realistic due to different hash algorithms used per tier depending on the architectures of the processor involved and hardware support, while also having alternate provisions for rare use cases where multiple hash algorithms may cause problems. The architecture shown here provides a unique level of flexibility and efficiency as well as security for IIoT.

5 Methodology

In order to find the most efficient way to implement blockchain for industrial applications, initially, we attempted to optimize the various algorithms in use to be as lightweight as possible. But soon we realized that there is a big drawback to such a method, due to the sheer range of computational devices in active use in an industrial environment with huge variation in computational power, ranging from a single-thread processor with very low clock speed to multi-microprocessor systems with hundreds of threads and several dozens of cores. While optimizing for the lowest common denominator for computational power is a valid option, it also creates a scenario where most of the computational power of the higher-powered devices remains unused. This wasted potential is counterproductive to our endeavour in search of efficiency.

Table 1 Comparison study of various hash functions

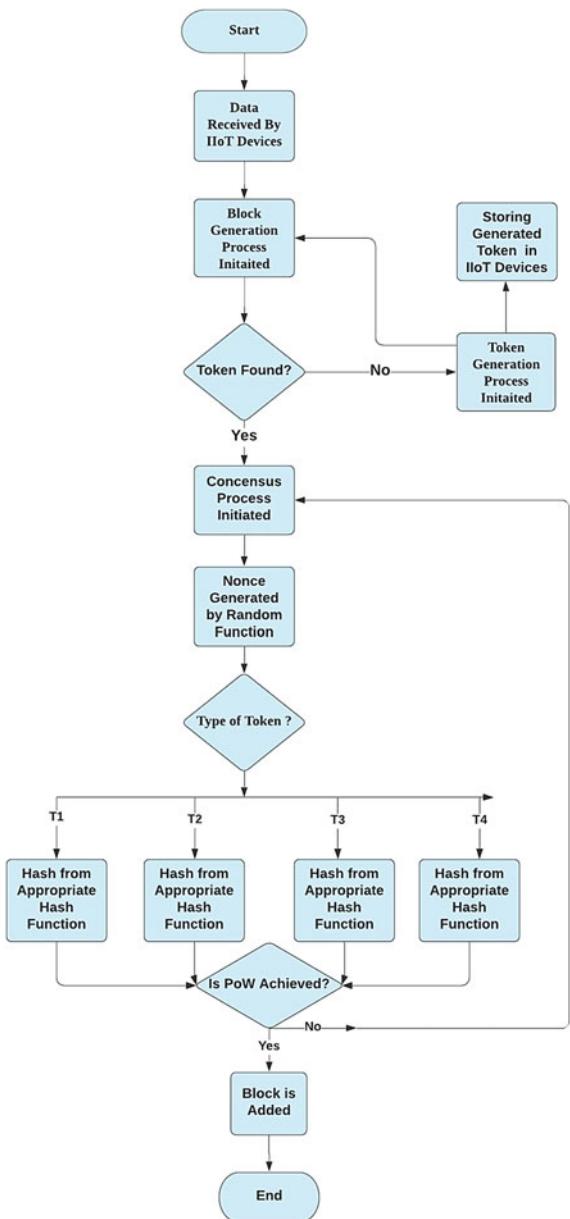
Algorithm	Type of attacks	Complexity	Block size	Word size	Output size
Blake2b [33]	Prefix collision	2^{256}	1024	64	512
	Prefix collision	2^{128}	512	32	256
MD2 [34]	Preimage	2^{128}	128	32	128
	Preimage	2^{128}	512	32	128
MD5 [36]	Preimage	2^{128}	512	32	128
	Collision	2^{128}	256	32	256
Panama [37]	Preimage	2^{128}	8	—	128
U-Quark [38]	Preimage	2^{160}	16	—	160
	Preimage	2^{224}	32	—	224
T-Quark [38]	Preimage	2^{64}	512	32	128
	Collision	2^{80}	512	32	160
RIPEMD-128 [39]	Collision	2^{64}	512	32	256
	Collision	2^{80}	512	32	160
RIPEMD-160 [40]	Collision	2^{64}	512	32	256
	Collision	2^{80}	512	32	160
RIPEMD-256 [40]	Collision	2^{64}	512	32	256
	Collision	2^{80}	512	32	160
SHA-0 [41]	Preimage	2^{160}	512	32	160
	Preimage	2^{512}	1600-2 * bits	64	Arbitrary hash length
SHA-1 [42]	Preimage	2^{256}	1088	64	256
	Preimage	2^{512}	576	—	512
SHA-3 (Keccak) [43]	Preimage	2^{80}	—	—	88
	Preimage	2^{208}	—	—	128
SHA256 [44]	Preimage	2^{256}	—	—	160
	Preimage	2^{512}	—	—	—
SHA512 [44]	Preimage	2^{80}	—	—	—
	Preimage	2^{208}	—	—	—
Spongent-88 [45]	Preimage	2^{120}	—	—	—
	Preimage	2^{208}	—	—	—
Spongent-128 [45]	Preimage	2^{120}	—	—	—
	Preimage	2^{208}	—	—	—
Spongent-160 [45]	Preimage	2^{120}	—	—	—
	Preimage	2^{208}	—	—	—

A simple processor benchmarking algorithm is being used to get a measure of the computational power of the IIoT devices being used, which in turn is used to generate the device token. This token is used for two specific purposes. Firstly, the device token contains tier data from the benchmarking algorithm which the block generation process uses to dynamically select the best fit for the hashing algorithm for the device's computational capacity. Next, this measure is also used to separate the various devices in the IIoT network into clusters each having devices of similar computational power.

There are many common ways to benchmark the processing power of a processor, such as finding a large number of prime integers, manipulating matrices of very large dimensions, and calculating factorials of large numbers. All of these approaches had one major issue. When the target value is set high, the required amount of time for the benchmark process to complete on devices with low power processors, like Raspberry Pi systems, becomes so high that it becomes unfeasible. When the target value is set low enough for low power devices to complete the process within feasible time, the result obtained from the benchmark algorithm became wildly inconsistent for the devices with higher power.

To solve these issues, we have chosen to create a new benchmarking algorithm, by iterating a number of complex trigonometric functions in fixed time. This time, T_{end} would remain fixed for all possible devices, so the number of iterations completed in this fixed time would vary positively with the computational power of the device concerned. This whole process is repeated R number of times and the mean number of completed iterations is used to gauge the computational power of the processor of the device. This mean is now used to generate the device-specific token, and this is depicted in the flowchart of Fig. 4.

The complex functions we have opted for are the following trigonometric functions: sine, cosine, tangent, and their inverse functions. All of these functions are relatively complex, having the same computational complexity $O(M(n)\log(n))$, where $M(n)$ being the cost of multiplication and n being the number of bits accuracy. Theoretically, the complexity of $M(n)$ itself is $O(n\log^2(n) \log \log(n))$ by Fourier's algorithm [46, 47]. There are a total of nine instances of these in the algorithm, executed over the full 360° range. For every reiteration N before the timer T reaches T_{end} , the total number of times the mathematical loop is repeated increases also by arithmetic progression by j which iterates from 1 to N. This ensures that for low power devices the total number of mathematical calculations remains low while increasing significantly for the higher power devices so that the end result is sufficiently consistent even if T_{end} is set to be quite low.

Fig. 4 Flowchart

Benchmarking Algorithm for Token Generation

Input- Computational Power of a Device

Output- Token

```

1: procedure Token Generation
2:   for i = 1 to Range, (incrementing i by +1) do
3:     initialise integer N as 1
4:     initialise Timer T
5:     calculate end time, Tend
5:     while T < Tend do
6:       initialise float V1, V2, V3 as 1
7:       for j = 1 to N, (incrementing j by +1) do
8:         for θ = 1 to 360, (incrementing θ by +1) do
9:           convert θ from degree to radians,
store as θr
10:          new V1 = old V1*sin(acos(sin2(θr)))
11:          new V2 = old V2*cos(asin(cos2(θr)))
12:          new V3 = old V3*tan(atan(tan2(θr)))
13:        end for
14:      end for
15:      increment N by +1
16:    end while
17:    store (N-1) values in Result []
18:  end for
19: Get mean = (1/Range) *( $\sum_{i=0}^{i=N-1}$  Result[i])
20: initialise Threshold [] = {Th1, Th2, Th3}
21: If mean < Th1 then
22:   return T1 token
23: else If mean < Th2 then
24:   return T2 token
25: else If mean < Th3 then
26:   return T3 token
27: else
28:   return T4 token
29: end If
30: end procedure
```

Algorithm for Token Generation

The token of the device is read by the consensus algorithm to gauge the computational power of the IIoT device in question, which now assigns the most efficient hashing algorithm available for that device. This hashing algorithm is used to create the hash of data of the block along with a nonce that is randomly generated. The hash generated is then subjected to a fixed target mathematical difficulty till Proof-of-Work is achieved or the block gets rejected. The process is shown below.

Hash Selection Algorithm:

Input- Block

Output- Hash of the block

```

1: procedure Hash Selection
2: If exist(token)=False then
3:   token = Token Generation ()
4: end if
5: if token == T1 then
6:   return Hash_Algo_1(block)
7: else if token ==T2 then
8:   return Hash_Algo_2 (block)
9: else if token ==T2 then
10:  return Hash_Algo_3(block)
11: else
12:  return Hash_Algo_4(block)
13: end if
14: end procedure
```

Algorithm for Hash Selection

Block Mining Algorithm:

Input- Block

Output- Chain of Blocks

```

1: procedure Block Mining
2: for n = 1 to Range, (incrementing n by +1 upto maxNonce) do
3:   if Hash Selection(block)<= target then
4:     add(block)
5:   else
6:     nonce_block = Random_nonce()
7:   end if
8: end for
9: end procedure
10: end if
11: end procedure
```

Algorithm for Block Mining

As previously mentioned, in certain use cases, the usage of multiple different hash functions within the same network can cause hindrances. In these use cases, an alternate process is used. In the consensus algorithm, there is no hash algorithm selection and a fixed hash algorithm is used for all tiers of devices. Instead, a target

selection algorithm is used within the consensus algorithm which assigns different mathematical difficulty targets to the different tiers of devices to best optimize the available computational power as shown in Table 5.

Target Selection Algorithm

```

1: procedure Target Selection
2: If exist(token)=False then
3:   token = Token Generation ()
4: end if
5: if token == T1 then
6:   Target=tar_1
7: else if token ==T2 then
8:   Target=tar_2
9: else if token ==T2 then
10:  Target=tar_3
11: else
12:  Target=tar_4
13: end if
14: end procedure
```

Alternate Algorithm for Target Selection

6 Implementation

The model proposed is used in a simulated plant for enhancing the safety and security of the plant. To test the storage of data securely in blockchain, we have built a simulation of a plant for IIoT using various smart devices of varying computational powers with numerous temperature and humidity sensors installed in motors for multipoint temperature sensing. Compared to existing systems, the proposed system delivers better performance in terms of enhanced security and faster performance. The sensors are used to monitor the temperature and humidity of motors for maintaining the safety of a plant. The system is advantageous and feasible to use for real-time data in an industry. The sensors chosen give accurate results, which are stored in blockchain at a comparatively faster rate as the hash function is being used according to the computational capability of a device. The selection of appropriate hash function helps in optimum usage of the computational power of a device and hence enhance the security of data stored in blockchain. We have run the token generation algorithm (benchmarking) over a range of devices with varying computational powers, using Python3 as our language of choice. For our test scenario, in the benchmark algorithm, we have set Range as 10 and T_{end} as 150 ms, for a total computational time of 1.5 s.

Every test was repeated 20 times and the results were very consistent and in line with what we expected. The output is shown in Table 2.

We have set the following thresholds for each tier based on the scores and have tested the following hash algorithms: Spongent-128, d-Quark, Blake2s, and Keccak256 by various devices of each tier, as detailed in Table 3. Deciding the hash algorithm for each tier was largely based on the experimental results we got by testing each tier of devices with 1000 sample blocks per hashing algorithm, which is discussed in the Result Analysis section. We used our consensus algorithm using a target difference of 15 for our test with Python3 as our language of choice. Figures 5, 6, 7, and 8 show the created blockchain in all four tiers of devices.

7 Result Analysis

We have created the experimental setup in a simulated plant for IIoT usage with a host of smart devices with varying computational power, numerous temperature, and humidity sensors installed in servo motors for monitoring multi-point data and storing it securely in blockchain to maintain the safety of the plant. The sensor data are collected for monitoring and help prevent overheating and ensure the safety and security of the plant. To analyse the efficiency of the implemented model, we created a statistical comparison of different algorithms per tier and compared our implementation results to the expectation of this statistic.

To find the optimum hash algorithm for each tier of devices, we have used 1000 sample blocks per tier for each hashing algorithm to find the expected computational time per block generated, with the exception of non-lightweight algorithms in the first two tiers, which were taking unfeasible times and hence ten samples were taken instead. A graph of benchmark scores of the various devices used in the IIoT simulation is given in Fig. 9. The resulting data of the tier-based hash algorithm comparison are shown in Table 4 and Fig. 10.

In Tier I, we have used the devices Redmi 2 Prime, Raspberry Pi 3B, Moto E cell phone for sampling data. For this tier of devices, Spongent-128 was providing us the best computational time per block at 2.91052278 ms, while d-Quark provided a relatively higher computational time per block at 3.40191614 ms, as seen in Table 7. More complex hash algorithms such as Blake2s and Keccak256 were taking significantly higher computational time per block at over 8 min per block, making them unfeasible for this particular tier of devices at our required target difference.

In the case of Tier II, the devices used for sampling are iPhone6s and Redmi Note 4. In these devices, we are getting very good computational time per block with both Spongent-128 and d-Quark at 1.44010181 ms and 1.49501915 ms, respectively. While Spongent-128 is slightly faster, d-Quark provides 80 bits of security over Spongent-128's 64 bits. The computational time per block of Blake2s and Keccak256 is still over 90 s in this tier and hence not viable for these devices.

For Tier III, we have used Microsoft Surface Pro 7 and Lenovo IdeaPad Slim 3. From this tier, the disadvantages of lightweight cryptography, primarily its lack

Table 2 Benchmark scores of different smart devices

Device type	Model	Processor	Benchmark score
Raspberry Pi	B+	700 MHz Single-Core ARM11	4
Raspberry Pi	2B	900 MHz Quad-Core ARM Cortex-A7	5
Raspberry Pi	Zero Wireless	1 GHz Single-Core ARM11	6
Cellphone	Moto E	1.2 GHz Dual-core Cortex-A7	7
Cellphone	Redmi 2 Prime	1.2 GHz Quad-Core 64-bit ARM Cortex A53	7
Raspberry Pi	3B	1.2 GHz Quad-Core 64-bit ARM Cortex A53	7
Cellphone	Canvas A1	1.3 GHz Quad-core Cortex-A7	8
Cellphone	Redmi 1S	1.6 GHz Quad-core Cortex-A7	8
Raspberry Pi	3A +	1.4 GHz Quad-Core 64-bit ARM Cortex A53	8
Raspberry Pi	4B	1.5 GHz Quad-Core 64-bit ARM Cortex A72	8
Cellphone	Xolo Play	1.8 GHz Quad-Core Nvidia Tegra 3 OC	9
Cellphone	Redmi 3	Octa-core (4 × 1.5 GHz Cortex-A53 & 4 × 1.2 GHz Cortex-A53)	10
Cellphone	iPhone 6 s	1.84 GHz Dual-core Twister	12
Cellphone	Redmi Note 6S	Octa-core (4 × 1.8 GHz Kryo 260 Gold & 4 × 1.6 GHz Kryo 260 Silver)	13
Cellphone	Redmi Note 4	2.0 GHz Octa-core Cortex-A53	14
Cellphone	iPhone 8	Hexa-core (2 × 2.39 GHz Monsoon + 4 × 1.42 GHz Mistral)	16
Laptop	Dell Inspiron 15 3542	1.7 GHz Dual Core Intel® Core™ i3-4005U	16.5
Cellphone	MiA2	Octa-core (4 × 2.2 GHz Kryo 260 Gold & 4 × 1.8 GHz Kryo 260 Silver)	17
Tablet	iPad Pro 12.9	Octa-core (4 × 2.5 GHz Vortex + 4 × 1.6 GHz Tempest)	17
Desktop	Custom Desktop	3.0 GHz Dual Core Intel® Core™ 2 Duo E8400	17.8
Cellphone	iPhone 11	Hexa-core (2 × 2.65 GHz Lightning + 4 × 1.8 GHz Thunder)	18

(continued)

Table 2 (continued)

Device type	Model	Processor	Benchmark score
Cellphone	Oneplus 8 T	Octa-core (1 × 2.84 GHz Kryo 585 & 3 × 2.42 GHz Kryo 585 & 4 × 1.8 GHz Kryo 585)	18
Tablet	iPad Air 4	Hexa-core (2 × 3.0 GHz Firestorm + 4 × 1.8 GHz Icestorm)	18
Desktop	Custom Desktop	3.8 GHz Dual Core AMD A6-7480	19
Laptop	Microsoft Surface Pro 7	1.3 GHz Quad Core Intel® Core™ i7-1065G7(Boost up to 3.9 GHz)	19
Laptop	Lenovo IdeaPad Slim 3	2.6 GHz AMD Ryzen™ 3 3250U(Boost up to 3.5 GHz)	20.2
Laptop	MacBook Pro M1	Octa Core Apple M1(Boost up to 3.2 GHz)	21.4
Laptop	MacBook Pro	2.3 GHz Octa Core Intel® Core™ i9-9880H(Boost up to 4.8 GHz)	21.9
Desktop	Custom Desktop	4.2GHz Octa Core AMD Fx 8350 OC	22.2
Laptop	Asus ZenBook Pro 15	2.9 GHz Hexa Core Intel® Core™ i9-8950HK(Boost up to 4.8 GHz)	22.4
Laptop	Asus ZenBook Pro Duo	2.9 GHz Octa Core Intel® Core™ i9-10980HK(Boost up to 5.3 GHz)	24
Desktop	Custom Desktop	4.9 GHz AMD Ryzen™ 9 5900X	26.5
Desktop	Custom Desktop	5.0 GHz Hexa Core Intel® Core™ i7-8700 K OC	27.8
Desktop	Custom Desktop	5.2 GHz Hexa Core Intel® Core™ i9-10900 K OC	29.2

Table 3 Hash algorithm used in different tiers of devices

Tier type	Device score	Algorithm used
Tier I	0–8	Spongent-128
Tier II	9–16	d-Quark
Tier III	16–24	Blake2s
Tier IV	24 +	Keccak256

```
-----  
Block Number: 3  
Block Data (Humidity and Temperature): [[[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]],  
[[62.0, 30.0], [62.0, 30.0], [61.0, 30.0], [61.0, 30.0]], [[61.0, 30.0], [61.0, 30.0], [62.0, 30.0], [62.0, 30.0]],  
[[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]], [[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]]]  
Block Hash: 339d05eda9f4eecd4269e75c63303c64  
Previous Hash: 7ec86000712c1f1a09f220999c221ad3  
Nonce: 3620669581  
Time stamp 2021-02-24 15:31:55.118626  
-----
```

```
-----  
Block Number: 4  
Block Data (Humidity and Temperature): [[[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]],  
[[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]], [[61.0, 30.0], [61.0, 30.0], [62.0, 30.0], [61.0, 30.0]],  
[[62.0, 30.0], [62.0, 30.0], [61.0, 30.0], [61.0, 30.0]], [[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]]]  
Block Hash: ca6a7ffccbf17468ab854877b8c663e95  
Previous Hash: 339d05eda9f4eecd4269e75c63303c64  
Nonce: 763283619  
Time stamp 2021-02-24 15:31:55.122615  
-----
```

```
-----  
Block Number: 5  
Block Data (Humidity and Temperature): [[[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]],  
[[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]], [[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]],  
[[62.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]], [[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]]]  
Block Hash: 7381739e44dcfa30353079856cdcb57a1  
Previous Hash: ca6a7ffccbf17468ab854877b8c663e95  
Nonce: 1368430752  
Time stamp 2021-02-24 15:31:55.124610  
-----
```

Computation Time per Block in ms: 3.0035680000000012
Hash Algorithm Used: spongeit-128

Fig. 5 Blockchain in Tier I device

```
-----  
Block Number: 3  
Block Data (Humidity and Temperature): [[[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]],  
[[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]], [[61.0, 30.0], [61.0, 30.0], [62.0, 30.0], [61.0, 30.0]],  
[[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]], [[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]]]  
Block Hash: 47e7e0ce725f615f94961df9061db452172e0a94  
Previous Hash: 1d21398f33dad48b7e1bcf59f2a8a11f6362346b  
Nonce: 1390783147  
Time stamp 2021-02-24 14:38:56.380760  
-----
```

```
-----  
Block Number: 4  
Block Data (Humidity and Temperature): [[[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]],  
[[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]], [[61.0, 30.0], [61.0, 30.0], [62.0, 30.0], [61.0, 30.0]],  
[[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]], [[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]]]  
Block Hash: fcfcfb580dfbd18eb367c7c4dd93336a248f989e  
Previous Hash: 47e7e0ce725f615f94961df9061db452172e0a94  
Nonce: 3846004895  
Time stamp 2021-02-24 14:38:56.382754  
-----
```

```
-----  
Block Number: 5  
Block Data (Humidity and Temperature): [[[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]],  
[[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]], [[62.0, 30.0], [61.0, 30.0], [62.0, 30.0], [61.0, 30.0]],  
[[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]], [[61.0, 30.0], [61.0, 30.0], [61.0, 30.0], [61.0, 30.0]]]  
Block Hash: 0d024cf1661a5ca7a514e4eae85cf28e94eaba2f  
Previous Hash: fcfcfb580dfbd18eb367c7c4dd93336a248f989e  
Nonce: 3667395859  
Time stamp 2021-02-24 14:38:56.384751  
-----
```

Computation Time per Block in ms: 1.4865181999999866
Hash Algorithm Used: d-Quark

Fig. 6 Blockchain in Tier II device

```

Block Number: 3
Block Data (Humidity and Temperature): [[[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [59.0, 28.0]], [[59.0, 28.0], [59.0, 28.0], [59.0, 28.0], [59.0, 28.0]], [[59.0, 28.0], [59.0, 28.0], [59.0, 28.0], [59.0, 28.0]], [[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]]]
Block Hash: f7744ce1fd3a9ad664cd09ee4fe103908024653c9218426e977053095ee973df
Previous Hash: e183f0919a5cc70a6c99dbdd8550fe843e0e2dc760fd13b1fe2ea13771e7fc
Nonce: 1567287249
Time stamp 2021-02-25 13:41:45.042722
-----
```

```

Block Number: 4
Block Data (Humidity and Temperature): [[[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]]]
Block Hash: e9b849d94802c37e1b2f93b9cc7fd726546115c8db257a7fdfc5ddd8aa9acc09
Previous Hash: f7744ce1fd3a9ad664cd09ee4fe103908024653c9218426e977053095ee973df
Nonce: 2303866936
Time stamp 2021-02-25 13:41:50.562964
-----
```

```

Block Number: 5
Block Data (Humidity and Temperature): [[[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [59.0, 28.0]]]
Block Hash: a0cc7145c80d3ef65b554c4a1b79c50e768a075d78ce07febd38acf5e3c413
Previous Hash: e9b849d94802c37e1b2f93b9cc7fd726546115c8db257a7fdfc5ddd8aa9acc09
Nonce: 2248313800
Time stamp 2021-02-25 13:42:05.628339
-----
```

Computation Time per Block in ms: 9344.6439188
Hash Algorithm Used: Blake2s

Fig. 7 Blockchain in Tier III device

```

Block Number: 3
Block Data (Humidity and Temperature): [[[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[60.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]]]
Block Hash: ccd67acd598174aae6558e3147c298d0e4f9e6e59ee5475b53e4417e97951cb
Previous Hash: b04c2a8bdd162ce86381c0241a18e3bc7d5887f4db648366561a22e8249baa19
Nonce: 2122494963
Time stamp 2021-02-25 16:17:35.059656
-----
```

```

Block Number: 4
Block Data (Humidity and Temperature): [[[59.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[59.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[59.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[59.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]], [[59.0, 28.0], [60.0, 28.0], [60.0, 28.0], [60.0, 28.0]]]
Block Hash: 0299194888a6e9285e02b423dbbf923e3f29d51964293818d6c95e897ba7b651
Previous Hash: ccd67acd598174aae6558e3147c298d0e4f9e6e59ee5475b53e4417e97951cb
Nonce: 2844033580
Time stamp 2021-02-25 16:17:35.239176
-----
```

```

Block Number: 5
Block Data (Humidity and Temperature): [[[59.0, 28.0], [59.0, 28.0], [59.0, 28.0], [59.0, 28.0]], [[59.0, 28.0], [59.0, 28.0], [59.0, 28.0], [59.0, 28.0]], [[59.0, 28.0], [59.0, 28.0], [59.0, 28.0], [59.0, 28.0]], [[59.0, 28.0], [59.0, 28.0], [59.0, 28.0], [59.0, 28.0]], [[59.0, 28.0], [59.0, 28.0], [59.0, 28.0], [59.0, 28.0]]]
Block Hash: 6f07a1b7cb2a2492a01a8410452f38f696e8a5b29ff7a538e0ffe6504ff9870
Previous Hash: 0299194888a6e9285e02b423dbbf923e3f29d51964293818d6c95e897ba7b651
Nonce: 1082646277
Time stamp 2021-02-25 16:17:35.470558
-----
```

Computation Time per Block in ms: 2062.9772365999997
Hash Algorithm Used: Keccak256

Fig. 8 Blockchain in Tier IV device

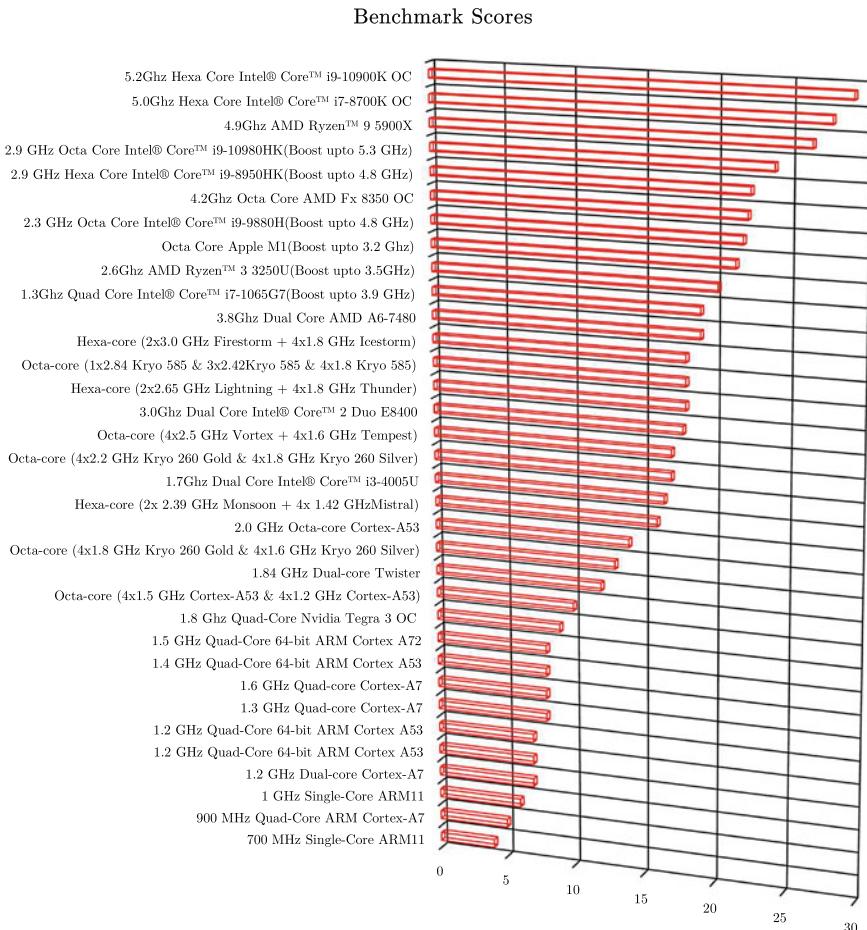


Fig. 9 Comparison of the computational powers of devices of different tiers

Table 4 Comparison of computational time per block generated of different hash algorithms for different tiers of devices

Hash algorithm	Computational time per block generated (ms)			
	Tier 1	Tier 2	Tier 3	Tier 4
Spongent-128	2.910523	1.440102	0.961031	0.841294
d-Quark	3.401916	1.495019	1.021349	0.894756
Blake2s	849,121.4	94,416.75	9349.722	2176.326
Keccak256	1,014,560	125,416.1	9718.491	2097.121

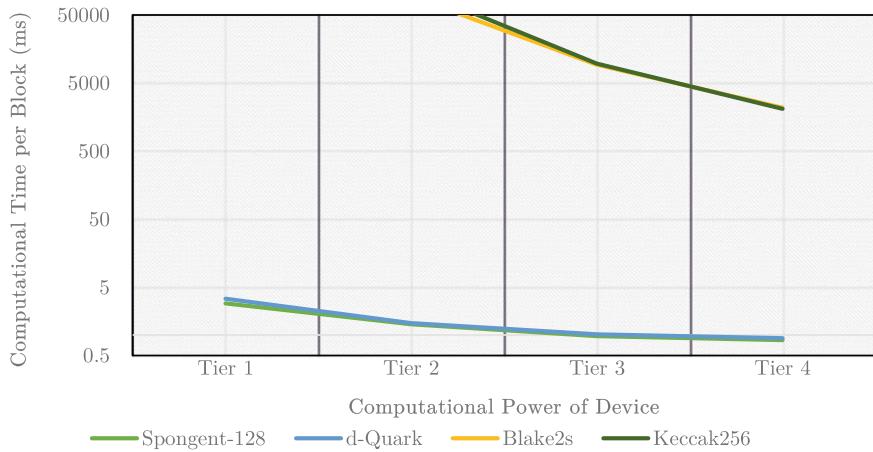


Fig. 10 Graphical comparison of computation time per block generated of different hash algorithms for different tiers of devices

of bandwidth starts becoming apparent. Also, lack of software support, as well as comparatively less security and restrictions, in its design makes it hard to optimize existing software for lightweight hash functions. The need for higher bandwidth thresholds and the additional security of more complex hash algorithms like Blake2s and Keccak makes them more suitable from this tier onwards with computational time per block less than 10 s. We opted for Blake2s, as it was very well optimized for devices of this tier, many of which use Intel Skylake processors, which is also reflected in the sampled data.

For Tier IV, two custom desktops with configurations (4.9 GHz AMD Ryzen™ 9 5900X, 32 GB RAM, Nvidia Geforce RTX 3080) and (5.0 GHz Hexa Core Intel® Core™ i7-8700 K OC, 16 GB RAM, Nvidia Geforce GTX 1060) are used in the sampling process. At this level of computational power, most secure algorithms will have very respectable computational time per block due to the abundance of processing power. We opted for Keccak256 in this tier based on the lowest computational time for 256 bits.

If we look back at the resulting output in our implementation from Figs. 5, 6, 7, and 8, we can see the computational time per block generated achieved in the simulation are as follows:

Tier I: 3.0035 ms, Tier II: 1.4865 ms, Tier III: 9344.6439 ms, Tier IV: 2062.9772 ms.

These values are well within of scope of the analytic results achieved in the statistical comparison of different algorithms per tier. Hence, our implementation of the proposed model of blockchain architecture is proven to be efficient for IIoT.

8 Performance Comparison

To compare the performance of our model of blockchain with existing blockchain models, we set up a peer-to-peer network using the following devices: Raspberry Pi 2B, Xiaomi Redmi 3, MacBook Pro M1, and a custom desktop with the processor AMD Ryzen™ 9 5900X fixed at a 4.9 GHz overclock. These devices have a huge variance in terms of computational power as seen in Fig. 9 and resemble a viable IIoT network. We implemented our proposed model of blockchain architecture within this network using a target difference of 15 and mined 100 blocks in each device. The average computational time per block mined is calculated for each device. This experiment is now repeated using the Bitcoin model of blockchain in this same P2P network using the same target difference. Again, the average computational time per block mined for each device is noted for the Bitcoin model. A comparison of the mean computational time per block mined for each specific device for both models has been given in Table 5. The mean computational time per block mined of the whole P2P network is compared for both models in Fig. 11.

From Table 5, it can be observed that our model has lesser computational time per block generated across all the devices in the network indicating a higher mining rate. Figure 11 shows that our proposed model takes less than 1% time on average

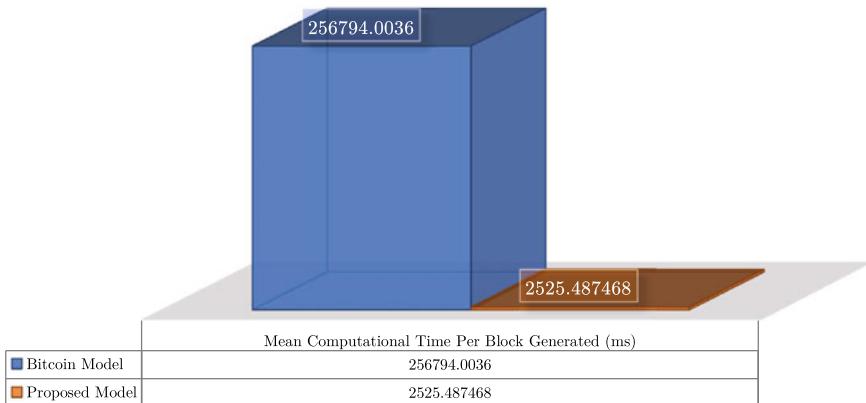


Fig. 11 Comparison of mean computational time per block generated between our proposed model and the bitcoin model over the P2P network

Table 5 Comparison of computational time per block generated between our proposed model and the bitcoin model

Implementation	Computational time per block generated (ms)			
	Raspberry Pi 2B	Xiaomi Redmi 3	MacBook Pro M1	Custom Desktop
Bitcoin model	901,536.0502	114,056.2563	9486.709635	2096.998156
Proposed model	2.719635	1.624886	8170.194398	1927.410954

for mining a single block in the IIoT network when compared to the Bitcoin model. It can be inferred from this observation that our proposed model is more than 100 times faster than Bitcoin for IIoT applications while maintaining a higher standard of security due to its inherent crypto agile design. This proves that our novel architecture of blockchain is significantly more efficient for usage in IIoT ecosystems.

9 Future Research Direction

Possible Research Areas:

- Further research on the pseudonymous nature of blockchain data and its possible implications from a privacy point of view is important.
- Proper device identification protocols without compromising privacy and security is a necessary research direction.
- The creation of proper lightweight cryptographic hash algorithms for use in IoT is necessary for the further development of IIoT-based blockchain architectures.
- Studying the effect of cryptanalytic attacks on IIoT-based blockchain models will further improve the security of these models.
- Fifth-generation communication technology (5G) in blockchain-enabled IIoT can provide new potential for IIoT.

Possible Workarounds of Security Vulnerabilities in IoT:

- Proper contingency methods and protocols to counter probable attacks in IIoT.
- Developing exclusive networks for usage in IIoT environments.
- Development of industry-standard protocols for management and security of IoT data with proper blockchain support as well as direct cloud integration.
- Efficient secure processing methods for maintaining the large amount of data produced in IIoT using blockchain.
- Developing AI-based preventive measures to detect possible intrusion in IIoT ecosystems.
- Creating DDoS and anomalous data detection systems.
- Lightweight methods to shield vulnerable IIoT devices from possible hardware-based exploits.
- Development of authorization schemes for anonymous, secure classification of devices in IIoT.
- Development of encryption methods suitable for IIoT to maintain integrity as well as the confidentiality of data during transfers within the network.
- Making existing IIoT methods natively compatible with blockchain.

Security-related Issues in IIoT:

- Designing efficient IIoT data communication systems to minimize feedback and transfer latency as well as decrease probable computation overhead on resource-constrained devices.

- Securing various cloud-based interactions for IIoT networks during data transfer and storage of data in clouds.
- Creating tamper-proof data transfer systems for low powered devices.
- Securing intra-network communications from cryptanalytic attacks.
- Developing proper decentralized, distributed systems for data management in IIoT ecosystems.
- Specific attack prevention mechanisms for devices of different architectures.
- Standardization of security protocols and policies for IoT ecosystems for industrial purposes.

Loopholes in blockchain-based IIoT:

- Lack of proper software support for blockchain-based systems in IIoT.
- High bandwidth needs for maintenance of blockchain-based IIoT ecosystems.

10 Conclusion

Blockchain-enabled IIoT networks are evolving at a very high pace. It is becoming a new standard in worldwide progress. The combination of blockchain and IIoT will bring huge technological leaps that will be able to bring remarkable enhancements to various facets of human life to make our society smarter and easier. In this chapter, the proposed model efficiently utilizes the computational power of the devices in the IIoT network to create a blockchain using the most suitably fitting hash algorithm. A new benchmarking algorithm is designed to be applicable on wide-ranging devices instead of computationally similar devices. This benchmarking algorithm helps to cluster the numerous devices in the IIoT network into different tiers. On the basis of the tier of a device, a computationally suitable hash algorithm is applied. Securing industrial IoT using efficient blockchain design enhances and expands IIoT applications. The above experimental result shows that the proposed model is efficient enough with respect to computational power, security enhancement, and energy utilization of the device in the IIoT network. To promote and expand the functions of IoT and IIoT platforms, various research and development projects are continuously conducted. Despite numerous efforts, in this developing field, there still exist some challenges and issues that are holding back the success of IoT in industrial environments. Since this field is still growing, it can be improved by proper directed developments. Hence, to guide future research in this domain some of the potential research challenges and open issues are discussed at the end of this paper.

References

1. Sharma N, Shamkuwar M, Singh I (2019) The history, present and future with IoT. In: Intelligent systems reference library, vol 154. Springer, Cham
2. Anagnostopoulos NA, Ahmad S, Arul T, Steinmetzer D, Hollick M, Katzenbeisser S (2020) Low-cost security for next-generation IoT networks. *ACM Trans Internet Technol* 20(3):31
3. Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK (2020) A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues. *IEEE Commun Surv Tutor* 22(2):1191–1221
4. Cano JC, Berrios V, Garcia B, Toh CK (2018) Evolution of IoT: an industry perspective. *IEEE Internet of Things Mag* 1(2):12–17
5. Raposo D, Rodrigues A, Sinche S, Sá Silva J, Boavida F (2018) Industrial IoT monitoring: technologies and architecture proposal. *Sensors* 18(10):3568
6. Sisinni E, Saifullah A, Han S, Jennehag U, Gidlund M (2018) Industrial Internet of Things: challenges, opportunities, and directions. *IEEE Trans Industr Inf* 14(11):4724–4734
7. Bakhshi Z, Balador A, Mustafa J (2018) Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models. In: IEEE wireless communications and networking conference workshops (WCNCW). Barcelona, Spain, pp 173–178
8. 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
9. Anand P, Singh Y, Selwal A, Alazab M, Tanwar S, Kumar N (2020) IoT vulnerability assessment for sustainable computing: threats, current solutions, and open challenges. *IEEE Access* 8:168825–168853
10. Khanna J, Sethi R, Sarangi P, Smruti R (2017) Internet of Things: architectures, protocols, and applications. *JF—J Electr Comput Eng* Hindawi
11. Pavithran D, Shaalan K, Al-Karak JN, et al (2020) Towards building a blockchain framework for IoT. *Clust Comput* 23:2089–2103
12. Wang Q, Zhu X, Ni Y, Gu L, Zhu H (2020) Blockchain for the IoT and industrial IoT: a review. *Internet Things* 10
13. Chatterjee R, Chatterjee R (2017) An overview of the emerging technology: blockchain. In: 3rd international conference on computational intelligence and networks (CINE). Odisha, India, pp 126–127
14. Khalid U, Asim M, Baker T, et al (2020) A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Clust Comput* 23:2067–2087
15. Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2019) LSB: a lightweight scalable blockchain XE “Lightweight Scalable Blockchain” for IoT security and anonymity. *J Parallel Distrib Comput* 134:180–197
16. Reyna A, Martín C, Chen J, Soler E, Díaz M (2018) On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener Comput Syst* 88:173–190
17. Doku R, Rawat DB, Garuba M, Njilla L (2019) LightChain: on the lightweight blockchain for the Internet-of-Things, pp 444–448
18. Liu Y, Wang K, Lin Y, Xu W (2019) LightChain XE “LightChain”: a lightweight blockchain system for industrial Internet of Things. *IEEE Trans Industr Inf* 15(6):3571–3581
19. J.Sousa, A.Bessani, M.Vukolic, “A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform”, pp. 51–58, 2018.
20. Ehmke C, Wessling F, Friedrich CM (2018) Proof-of-property: a lightweight and scalable blockchain protocol. In: Proceedings of the 1st international workshop on emerging trends in software engineering for blockchain, pp 48–51
21. Seok B, Park J, Park J (20169) A lightweight hash-based blockchain architecture for industrial IoT. *Appl Sci* 9
22. Zamani M, Movahedi M, Raykova M (2018) RapidChain: scaling blockchain via full sharding, pp 931–948
23. Seok B, Park J, Park JH (2019) A lightweight hash-based blockchain architecture for industrial IoT. *Appl Sci* 9(18):3740

24. Huang K, Tso R (2012) A commutative encryption scheme based on ElGamal encryption, pp 156–159
25. Fu J, Qiao S, Huang Y, Si X, Li B, Yuan C (2020) A study on the optimization of blockchain hashing algorithm based on PRCA. *Secur Commun Netw* 1–12
26. Pissinou AS, Staier N, Kwan C (2019) Sensor-chain: a lightweight scalable blockchain framework for Internet of Things
27. Kiayias A, Russell A, David B, Oliynykov R (2017) Ouroboros: a provably secure proof-of-stake blockchain protocol. In: Annual international cryptology conference. Springer, Cham, pp 357–388
28. Dorri A, Kanhere S, Jurdak R (2017) Towards an optimized blockchain for IoT
29. Banafa A (2017) IoT and blockchain convergence: benefits and challenges. *IEEE Internet of Things*
30. Liu M, Yu FR, Teng Y, Leung VC, Song M (2019) Performance optimization for blockchain-enabled industrial Internet of Things (IioT) systems: a deep reinforcement learning approach. *IEEE Trans Ind Inform* 15(6):3559–70
31. Misra S, Mukherjee A, Roy A, Saurabh N, Rahulamathavan Y, Rajarajan M (2021) Blockchain at the edge: performance of resource-constrained IoT networks. *IEEE Trans Parallel Distrib Syst* 32(1):174–183
32. Stevens M, Bursztein E, Karpman P, Albertini A, Markov Y (2017) The first collision for full SHA-1. In: Annual international cryptology conference. Springer, Cham, pp 570–596
33. Aumasson JP, Neves S, Wilcox-O’Hearn Z, Winnerlein C (2013) BLAKE2: simpler, smaller, fast as MD5, vol 7954. Springer, Berlin
34. Thomsen SS (2008) An improved preimage attack on MD2, p 89. IACR Cryptol. ePrint Arch.
35. Leurent G (2008) MD4 is not one-way. In: International workshop on fast software encryption. Springer, Berlin, pp 412–428
36. Sasaki Y, Aoki K (2009) Finding preimages in full MD5 faster than exhaustive search. In: Annual international conference on the theory and applications of cryptographic techniques. Springer, Berlin, pp 134–152
37. Daemen J, Van Assche G (2007) Producing collisions for PANAMA, instantaneously. In: International workshop on fast software encryption. Springer, Berlin, pp 1–18
38. Aumasson JP, Henzen L, Meier W, Naya-Plasencia M (2013) Quark: a lightweight hash. *J Cryptol* 26(2):313–339. (Springer)
39. Wang X, Feng D, Lai X, Yu H (2004) Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD, p 199. IACR Cryptol. ePrint Arch.
40. Mendel F, Pramstaller N, Rechberger C, Rijmen V (2006) On the collision resistance of RIPEMD-160. In: International conference on information security. Springer, Berlin, pp 101–116
41. Manuel S, Peyrin T (2008) Collisions on SHA-0 in one hour. In: International workshop on fast software encryption. Springer, Berlin, pp 16–35
42. De Canniere C, Rechberger C (2008) Preimages for reduced SHA-0 and SHA-1. In: Annual international cryptology conference. Springer, Berlin, pp 179–202
43. Song L, Liao G, Guo J (2017) Non-full Sbox, linearization: applications to collision attacks on round-reduced keccak. In: CRYPTO. Springer, Cham, pp 428–451
44. Aoki K, Guo J, Matusiewicz K, Sasaki Y, Wang L (2009) Preimages for step-reduced SHA-2. In: International conference on the theory and application of cryptology and information security. Springer, Berlin, pp 578–597
45. Bogdanov A, Knezevic M, Leander G, Toz D, Varici K, Verbauwhede I (2012) Spongent: The design space of lightweight cryptographic hashing. *IEEE Trans Comput* 62(10):2041–2053
46. Brent RP (1976) Fast multiple-precision evaluation of elementary functions. *J ACM (JACM)* 23(2):242–251
47. Brent RP, Zimmermann P (2010) Modern computer arithmetic, vol 18. Cambridge University Press

Quantum Aware Distributed Ledger Technology for Blockchain-Based IoT Network



Koustav Kumar Mondal and Deepsuhbra Guha Roy

Abstract A digital ledger which is based on distributed technology will help to address cybersecurity and secrecy problems in the Internet of Things Architecture, but combining these two technologies poses some difficulties. In order to preserve a tradition of financial transactions, cryptocurrencies introduced DL technology. The DL size in a cryptocurrency addresses hundreds of GBs, while the storage of IoT nodes is limited. Similarly, cryptocurrencies implement costly processes of consensus, while IoT nodes in calculation and energy are restricted. Moreover, classic distributed ledger technology (Bitcoin) are not based on quantum. The chapter aims a distributed ledger security based on quantum technology, specifically distributed ledger for Internet of Things, for IoT architectures. One cornerstone of the chapter is a new signature creation scheme which is named as Single time signature based on time(STS), Blockchain-STS, a compact scheme. Compared with the famous Winteritz-OTS+ system Blockchain-STS offers a 75% reduction in signature size and a 76% reduction in signature generation time.

Keywords Quantum cryptography · Distributed Ledger (DL) technology · Internet of Things (IoT) · Post quantum digital signature · Cryptocurrency · Cloud computing

1 Introduction

IoT uses embedded technology for connecting and communicating material things. As a massive amount of material things are interconnected, a large amount of data is therefore generated. Maintenance of information protection and privacy remains a

K. K. Mondal

School of Computational Science, Department of IT, Maulana Abul Kalam Azad University of Technology, Simhat, Haringhata, Nadia, Kolkata, West Bengal 741249, India

D. Guha Roy ()

Mobile and Cloud Lab, Institute of Computer Science, University of Tartu, Ulikooli 17-324, 50090 Tartu, Estonia

tough job for IoT Architecture [1]. The “Things-Network” framework signifies a four-stage design, Sensor Layer, Networking Layer, Service (Blockchain or Cloud) Layer, and an Interface Layer (applicability programs) [2]. The Sensing Layer incorporates devices (actuators and sensors) integrated into the physical objects for communication. The sensor data are transmitted to S3 data storage of cloud through the Layer of Network. S3 Storage stores information and enables apps to start their processing the information in order to make human and living being more manageable. Figure 1 demonstrates layered IoT-based systems architecture [3]. In general, IoT devices lack storage, energy (battery life), and computing power. In general, sensor-formed data is collected in Clouds. Nevertheless, stability, privacy, and data reliability challenges arise in IoT systems [4, 5]. The transfer of large volumes of information to the Cloud causes an overload of network sources. Likewise, a malicious Cloud can damage data protection and privacy [6].

The corresponding IoT systems could be pushed out of operation to an idle status [7]. Distributed ledgers (DLs) present an appropriate cloud service alternative for IoT systems [8]. Instead of collecting information on a primary server, matches themselves store information. Each match controls a database nearby, although modifications to the data are done through mutual agreement between the peers [9]. The model of the information on each match is synchronized at all times. Although a

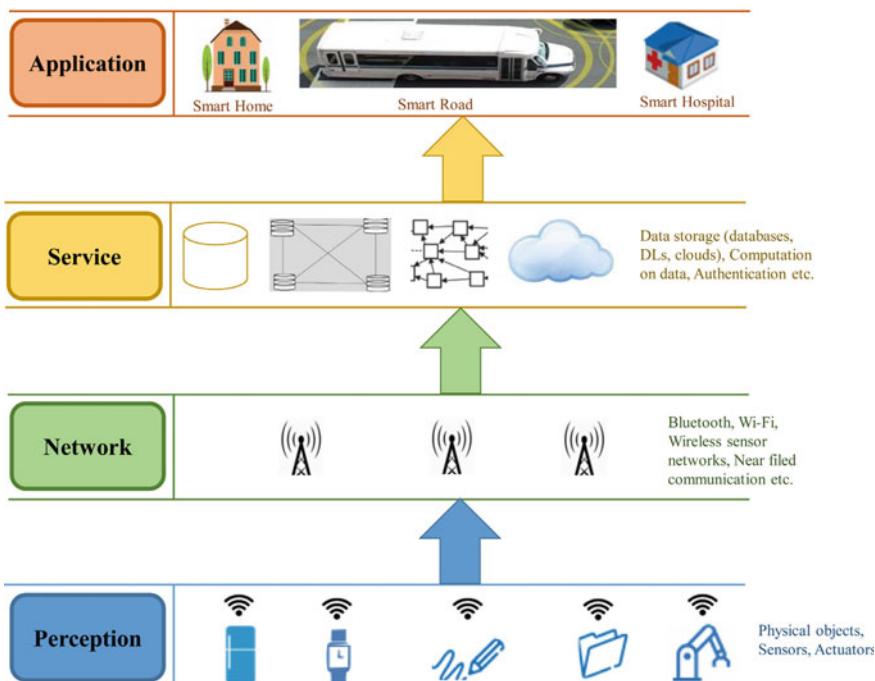


Fig. 1 Four-layered architecture of Internet-of-Things based working system

number of blockchain (DL) IoT systems are available, such as [10, 11], etc., there is still no widely accepted framework [7, 12]. The DL was initially suggested by cryptocurrencies (Bitcoin) to preserve a history of economic transactions. Nevertheless, it creates unusual difficulties by adopting DL technology for IoT-based operations. First of all, transactions are heavily linked to an input/output relationship in a cryptocurrency. Any new transaction would redeem the coins before locked by a traditional transaction. Though the transaction contents differ from the cryptocurrency in an IoT setting. A model of an IoT performance is the data produced by a sensor. The linkage of transactions of IoT to a legitimate string is. Therefore, a problem for IoT-based DLs [4]. Second of all, in a cryptocurrency, the size of a DL usually is quite big (as an example, the current volume of the Bitcoin ledger is around 200 GB), but IoT connections are restricted into stock. Third, DLs implement a computer-based cost-effective consent technique like ethereum's consensus algorithm (Proof-of-Work) to enable new operations or data block to be added to the repository. As IoT devices are energy and computation-limited, they are not suited to PoW-like consent mechanisms [13]. In one end, the Digital signature design applied through the classic DLs (such as Ethereum, Bitcoin) is the elliptic curve, which is not a quantum-safe algorithm [14]. The famous Shor algorithm allows an opponent to break ECDSA by a quantum computer that is sufficiently efficient [15]. DL technology will revolutionize IoT, but the convergence of two technologies presents challenges [7, 16]. Before the combination of the pair technologies, the related problems need to be carefully regarded. These difficulties are due to IoT gadgets that do not have the required calculation, communication, storage, and energy [5]. While blockchain-based IoT applications become suggested, such as [5, 10, 13, 17], it remains, however, an emerging research field without a widely accepted framework [7]. IoT systems cannot hold loads of consensus-like PoW structures. In addition, IoT devices cannot support a constantly increasing leader scale [18]. Finally, the digital signature system applied through the standard DLs is not immune to quantity [14]. For IoT-based systems, we discuss a quantum-secure DL, Blockchain-for-IoT, in this chapter. The DL proposed, recognizes, and discusses various issues related to Distributed Ledger technology adoption for IoT methods. We tackle four trials: Quantum Resilient Signature (QR), Scalability Ledger (LS), Transaction Chaining (TC), and Lightweight Consensus (LWC). This chapter developed the aimed Blockchain for IoT using a new STS scheme, Blockchain-STS, a lightweight, energy-efficient, and fast STS.

The chapter was structured as follows: Part 2 comprises the corresponding work. Part 3 outlines our design frame. Part 4 contains the STS scheme for DL construction. In Part 5, a quantum-safe DL for IoT operations is discussed, and Parts 6 and 7 assess the safety and success of our plans. Lastly, Part 8 ends with valuable guidelines for the future study.

2 Related Work

This portion comprises two paragraphs. Section 2.1 offers a description of DL technology-incorporating IoT applications. Section 2.2 gives a summary of current SHA384 hash-based STS technique's.

2.1 *Distributed Ledger-Based Internet of Things Network*

This section gives a provisional overview of research integrated with IoT technology by blockchain/DL. The DL technology extends well beyond cryptocurrencies [19]. Besides cryptocurrencies, in the development of intelligent agreements, Access Control Systems [20], healthcare, e-business, applications [21], VANETS [22], smart homes, intelligent cities [23], and so on, DL technology was also used. The Smart Access Control System [20] from Blockchain intends a design for IoT device management. The resourceful link, the management center, on the recommendation of the restricted IoT nodes [24], communicates with the Blockchain (i.e., sensor). An operator node creates the intelligent deal. The research does not have a mechanism for cutting boards and does not recommend any protection against quantum threats. Lightchain [13] aims at multiple synergistic proofs (SMP), a slight consent mechanism, and a UBOF, a ledger pruning mechanism. Lightchain [13] proposes an SMP. However, no ordinance for binding transactions into an internal or external exchange have been suggested or any protection upon quantum attacks. IOTA [4] is an intelligent cryptocurrency that serves the economy of machine-to-machine (M2M). In contrast to IOTEX, IOTA eliminates the costly technique's of consent (i.e., PoW). The Blockchain algorithm that IOTA uses is called the Tangle. A cutting mechanism is implemented to keep the leader size from continuously increasing. IOTA is using a secure signature system based on quantum technology (i.e., Winternitz OTS+). DL's intelligent house [23] concurrently uses two records, a regional immutable (IL) ledger and a public Blockchain [25]. The study does not propose any ledger cutting mechanism or quantity-attack protection. Lee and Lee suggested a Blockchain-based clarification to update embedded IoT device's firmware in a safe manner [26]. Each request for firmware upgrade erases a current block in Blockchain. The aimed leaflet has a computationally costly consensus mechanism and no leaflet cutting device. Blockchain-based VANETs enable VANETs to be increased and safety event messages disseminated efficiently [22]. The Blockchain [22] suggested is a local Blockchain that stores road cases information for the particular geographical area. The introduced Blockchain uses a costly consent system based on PoW and proposes no protection from quantum threats. An IoT-based E-business model was introduced by Zhang et al. using Blockchain technology [21]. The model proposed does not resolve the challenges of combining DL technology and IoT, such as the growing size of the leads and a highly costly consensus process [27, 28]. The latest Blockchain-based IoT purposes are summarized in Table 1.

Table 1 Blockchain-based IoT application's summary

Ref.	IoT Application	Transaction type	Smart contract	Mining	Sig. scheme	QR ^a	IoT-challenges		
							LS ^b	TC ^c	CM ^d
[12]	Access control	Triggered operation	Allowed operations	Miner nodes	ECDSA	x	x	x	PoC
[7]	IoT	Sensor data	x	ECS	ECDSA	x	UBOOF	x	SMP
[8]	Smart home	Tiers communication	x	CH	Non QR	x	x	/	DT ^e
IoTA [3]	Cryptocurrency	Financial transaction	x	All peers	WOTS	/	/	/	CC ^f
[13]	Firmware update	Update request	x	IoT nodes	ECDSA	x	x	x	PoW
[9]	VANETS	Safety events	x	Vehicles	Non QR	x	CB ^g	x	PoW
[16]	E-business	Financial transaction	Trade deals	Miners	ECDSA	x	x	/	PoW

^a Quantum resilient.^b Ledger scalability.^c Transaction chaining.^d Consensus mechanism.^e Distributed trust.^f Central coordination.^g Country-based.

2.2 SHA384 Hash-Based STS Technique

A well-known researcher Lamport Diffie suggested the signature sizes and comprehensive key for the first STS system. The Winternitz-OTS scheme (WOTS) provided reductions in main and signature sizes of 87% and 75% compared with the Lamport scheme. WOTS PRF and WOTS+ [11] are two lightweight WOTS alternatives that give a reduction in the signature size of approximately 33% in comparison with WOTS. HORS is an effective OTS system with minimal signature size. The major scale of HORS is, however, virtually bigger. Tree HORS (HORST) [10] compromise key size execution speed. PORS/PORST [29] are safer HORS/HORST variants.

2.3 IoT-Related Emerging Trends In Research

Apart from IoT DLs, several of the emerging IoT analysis trends contain adopting Green IoT communications designs using the 5G networks [30], Industrial surveillance applying large Data Analysis [17, 31], Big Data Analytics design of small businesses [32], modeling and optimizing social Internet selection features [33] defining the use of bi-based human behavior [34].

3 Discussion on System Model

The framework template proposed includes four layers (Fig. 2), Layer of Perception, Layer of Communication peer to peer, Network Layer based P2P technology, and Blockchain layer. The layer of perception reposes of driving/sensing gadget correlated to everyday household appliances(such as fridge, smart clock, bicycle), which enable them to interact. The layer of perception tools have minimal calculation and storage capacities [35]. The P2P layer is made up of peers that are capable of computer connections (like laptops or PCs). The pairs remain linked to each other and

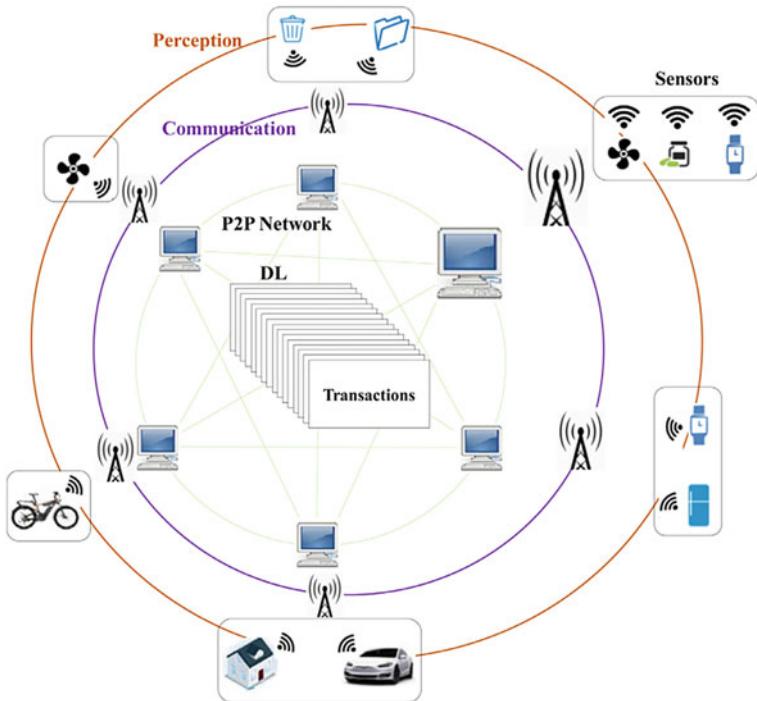


Fig. 2 System architecture model for Blockchain-based Internet of Things

thus form the P2P network. Individual peer has sufficient storage and computing capability to control a Distributed Directory (DD). The layer of communication provides communication among sensor peers and devices. Lastly, the records storage facilities are provided in the DL Layer. The matches preserve information on behalf of actuators and sensors in the aimed Blockchain-based IoT system [36]. Several actuators and sensors are attached to each peer. When information from one of the relevant sensors is received, a match creates a new deal and conveys it across the P2P network. Different peers validate the performance and collect the new deal in the ledger after reasonable verification (DL). We suggest a method that will assure that a new transaction can be stored in DL only by trusted peers. For a DL integrated into an IoT context, we have developed new transaction verification rules. The aimed transaction confirmation laws allow the DL to connect input/output deals. Therefore, each transaction has precisely one predecessor and one successor, “zero or one.” To succeed in an actual transaction a, the Signs of b must validate a key earlier collected in a. The transaction owner b (Owner B) may only sign the transaction later than the transaction owner a (Owner A). In this process, Owner A serves as Owner B’s sponsor. The consent given through the owner of an earlier collected transaction for each new transaction removes the need for a traditional (PoW) process. Therefore, we need not encapsulate single transactions within blocks, so our introduced DL

is a transaction store, not a block set. Specific transaction collects a slipping key so that the transaction owner can delete the activity until it is no longer necessary. The cutting key enables matches to periodically cut the record by removing wasteful activities following the agreement of respective admins. Matches are capable data nodes, and individual peer which connected to node locally collects the booklet. Nevertheless, a peer with unusual storage ability is not allowed to store the booklet locally. Since our modeling offers a board cutting mechanism, which enables pairs to eliminate unnecessary transactions safely, the board is therefore compact enough to store a pair with a standard storage capacity when needed.

3.1 Basic Elements in System Model

In our device model, there are three essential elements:

1. Physical items and embedded sensors (such as vehicles, refrigerators, portals, coffee makers).
 2. The connectivity medium for transferring information amongst physical items and Computing Nodes.
 3. The Network which have peer to peer technology capable of Computing Nodes, Hereabouts we describe the working function of every entity individually.
- **Embedded Sensors/Actuators Physical Things:** The layer of perception of the IoT architecture is clear. The built-in sensors transform physical environments into appropriate digital types. Digital signals are transformed by actuators into physical action. For example, an in-car sensor shows a digital atmospheric temperature and the actuator drives the coffee maker when a computer gets Digital Signals. Simply put, the actuators and sensors enable material objects to feel, interact, and carry out activities to help people live.
 - **Communication Medium:** The communication medium serves the IoT architecture network layer. Method of communication includes devices that enable data transmission between computing nodes and sensors/actuators. Communication equipment can contain BLE, Wireless Fidelity, NFC, and WSN.
 - **P2P Network:** a Peer-to-Peer network is a system of capable computer data nodes that implement two-tier Internet of Things architectural services, i.e., the Service and Application Layers. Matches (computer connections) obtain and method data from physical objects and take adequate measures to meet user conditions. The pairs manage a DL to collect the information transmitted through the sensors. Every peer keeps a model of the ledger. The safety and authenticity of the ledger are guaranteed by a new STS, i.e., Blockchain-STS. The sensor data is collected as transactions in the ledger. The effective peer generates a new activity and conveys it to another peer when a sensor transmits data. All other pairs check transactions (using the introduced STS scheme) and later collect them in the leader. When a current transaction shows that the machinery part should be started, the analogous peer acts his role and instates the relevant machine.

4 STS Scheme

Our suggested Blockchain-for-IoT is built on a hash-based single time signature structure. This segment describes in detail the introduced STS system. Our stated SS design has been denominated Blockchain-STS, the compactest and most successful scheme compared to all present STS plans. This sector will be restricted to the Blockchain-STS characteristics, while in Sect. 7, we will compare Blockchain-STS with current standard STS systems. Blockchain-STS is a fourfold version (key generation, signature, check, and key-compression). Key generation allows an input protection parameter (n) and delivers a key combination (sk, pk). Sign acquires the information (m) as the information furthermore delivers m signatures, i.e., σ^m with the private key(sk) Verify accepts input (m), $m(\sigma^m)$ signatures and the public key (pk), returning one of both outputs; unless prosperous or abandoned. Keycompress cryptographically compresses the public key.

4.1 Key Generation

This paragraph discusses the process of key creation toward our introduced STS system, Blockchain-STS. Within hash-based STS programs, several values are the key and the signature (denoted as l). The key and the signature at Blockchain-STS is a total of 17 values, 16 of which match the possible alphabets of a message hash to signify contracted, i.e., 0, 1, 2 and 17 for a checksum (quite similar WOTS including its alternatives utilize checksum). In addition, in STS systems, several iterations of hash (w) require the transition of an individual private key (sk) into a specific public key (pk). Each sk -value (except for the 17th value) of Blockchain-STS is 47 times (we decided 47 based on our analyses in the design of Blockchain-STS) for the corresponding pk -value to be produced. For “ l om w ” times (we refer to it as w_c), the 17th sk -value (it is utilized for MD5 Checksum) hashed toward the identical pk -value. Blockchain-STS recommends that each sk imports are produced from one fundamental importance called a handshake. We suggest using SHA384 for an increasing the security using post-quantum technology. In the entire post, we utilize H to relate to the SHA384 hash purpose. Table 2 illustrates the various symbols in this section and the following pages.

$$\begin{aligned} \sum_{i=1}^l sk_{i-1} &= H^i(seed) \\ \left[\sum_{i=0}^{l-2} pk_i = H^w(sk_i) \right] \cup [pk_{l-1} = H^{w_c}(sk_{l-1})] \end{aligned}$$

Table 2 Mathematical symbols and their description

Symbol	Description
l	No. of values in key/signatures
n	Bit-length of an individual key/signature value
h_m	Hash of the message to be signed
l_k	No. of values in key
w	No. of hash iterations used to transform an sk-value to the corresponding pk-value
w_c	Number of hash iterations used to transform the last sk-value (used for checksum) to the corresponding pk-value
sk_i	An individual value in private key
pk_i	An individual value in public key
PK	The compressed public key
H	Hash function SHA384
$H^n(m)$	SHA384 applied on m for n times
σ^m	Signatures created on message m
vk	Verification key computed by the verifier from the signatures (to be compared with pk)
$trxi$	i^{th} transaction stored in the ledger
$prnKey$	Pruning key (a PK to authorize a peer to remove an un-necessary transaction from DL)
$succID$	The ID of the transaction $trxi$ stored in the transaction $trxi_{i-1}$
\mathcal{F}	A forger who accepts the challenge to break DL-OTS
\mathcal{A}	An adversary who accepts the challenge to break oneway-ness of H
m^Q	Message queried by the \mathcal{F}_{DL-OTS} during the attack process
m^F	Message returned by the \mathcal{F}_{DL-OTS} at the end of the attack process

4.2 Signature Creation

Every method of development of signatures starts with a hash of the signed message (i.e. $h_m = H(msg)$). In its hexadecimal representation, we process message-hash. Since we use SHA384, h_m is comprised of 96 hexadecimal symbols (Eq. 4.2). The symbols are indexed as one to ninety-six. Then we group the records according to their symbols, as follows: The index set containing symbol 0; the index set containing symbol 1; up to the index set containing symbol F (Algorithm 1 steps 1–3). Then, in each of the 16 sets, we calculate a total of 16 integer values (steps 4–5). We utilize module operators to ensure all 17 values range from 1 to w (step 6). We calculate a check-sum for the above sixteen values in the next level: we extract each of the 17 w values and summarize all those differences (steps 7–8). Subsequently, we produce message signatures by computing post-images with the initial value “l-1”, numbers of terms the identical integer value (step 9). However, the ultimate sign component is created by calculating the post-image number of times the check-sum of the l th sk-element (step 10). Figure 3 illustrates the process of creating signatures with an example.

$$h_m = \sum_{i=1}^{96} m_i = \{m_1, m_2, \dots, m_{96}\}$$

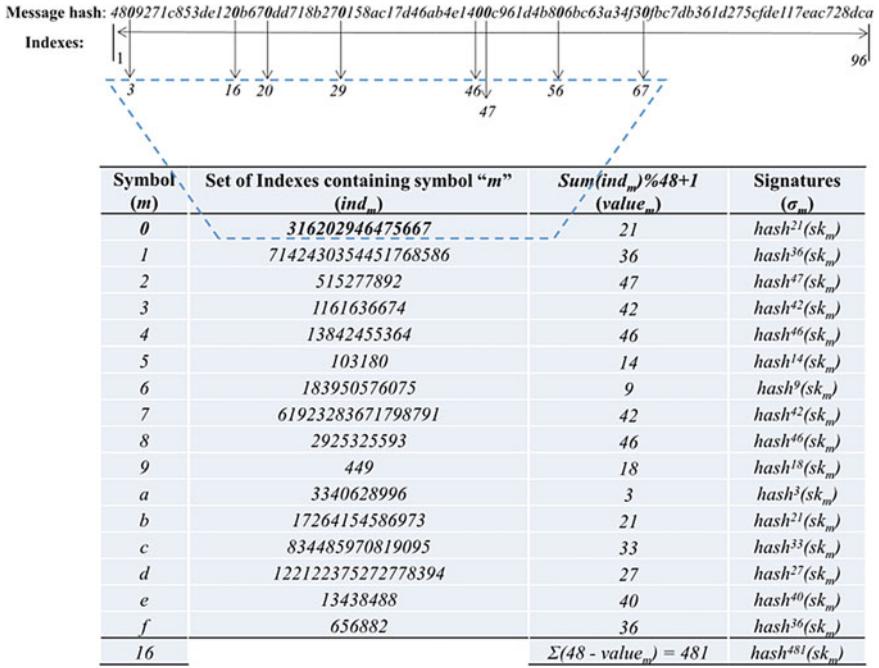


Fig. 3 Creation of the Blockchain-STS signature for an example ‘Good Message 707070’

Algorithm 1: Blockchain-STS. sign().

Input: $h_m, [sk_0, sk_1, \dots, sk_{l-1}]$

Output: $[\sigma_0, \sigma_1, \dots, \sigma_{l-1}]$

- 1: $\sum_{i=0}^{l-2} [ind_i \leftarrow \phi]$
 - 2: $j \leftarrow 1$
 - 3: $\forall x \in h_m \bullet \left[[ind_x \leftarrow ind_x \cup j] \wedge [j \leftarrow j + 1] \right]$
 - 4: $\sum_{i=0}^{l-2} [value_i \leftarrow 0]$
 - 5: $\sum_{i=0}^{l-2} \left[\forall d \in ind_i \bullet (value_i \leftarrow value_i + d) \right]$
 - 6: $\sum_{i=0}^{l-2} [value_i \leftarrow (value_i \% w + 1)]$
 - 7: $checksum \leftarrow 0$
 - 8: $\sum_{i=0}^{l-2} [checksum \leftarrow checksum + (w - value_i)]$
 - 9: $\sum_{i=0}^{l-2} \left[\sigma_i \leftarrow H^{value_i}(sk_i) \right]$
 - 10: $\sigma_{l-1} \leftarrow H^{checksum}(sk_{l-1})$
-

4.3 Verification of Signature

This verifier shall also take Algorithm first steps (1–8) in the signature verification to calculate the 16 conditions and the checksum. Subsequent the verifier can calculate the quantity of “w times” (each identical content) after each of the first “ $l - 1$ ” $\sigma - elements$. Verifier will also retrieve the post image number of times for the l th – element, $w_c - checksum$. The checker thus calculates total l values; we mark this collection of conditions as the check key [vk] (Eq. (4.3)). Ultimately, several calculated values will be compared to each identical pk-value. If the total conditions are the same, signatures (Eq. (4.3)) shall then be accepted by a verifier; otherwise, the signatures would be refused and null.

$$\left[\sum_{i=0}^{l-2} H^{w-value_i}(\sigma) \right] \cup [vk_{l-1} = H^{w_c-checksum}(\sigma_{l-1})] \\ \left[\sum_{i=0}^{l-1} vk_i == pk_i \right] \Rightarrow "Accepted"$$

4.4 Key Compression

The simple public key comprises 1 conditions, all 384-bit in length. We utilize the algorithm of Merkle hash tree to compact the available key to simply one long 384 -bit value. Figure 4 explains the compression tree structure, while Algorithm 2 explains in-depth the primary compression process. The simple pk consists of a total of seventeen hash values. Blockchain-STS utilizes a pure hash tree from Merkle to compress a single pk. Step 1 determines array N of height 4. Here, N is 31. In a perfect binary tree, there are 16 leaf nodes (of length 4). Step 2 reserves the values of definite pk in every N leaf node. The definite pk is formed by seventeen conditions, 16 of which remain consolidated under the N leaf nodes (the 17th value is integrate and hashed, including the node N which is a root node). At step 3 starts with a new variable j to run the outward circle (steps 4–9). The outward circle emphasize to the height of every tree for many cycles. Individually, renewal of the outer circle produces a novel overhead tree level. The internal loop (steps 6–8) is equivalent to the corresponding stage’s node for several cycles. Each inner loop iteration calculates a new tree node. We concatenate the two descendant nodes and calculate their hash to calculate a new parent node (step 7). Ultimately, in step 10, the tree root (N) is linked together among individual ending pk-values; furthermore, its hash is calculated. The value calculated within step 10 is the pk (indicated as PK).

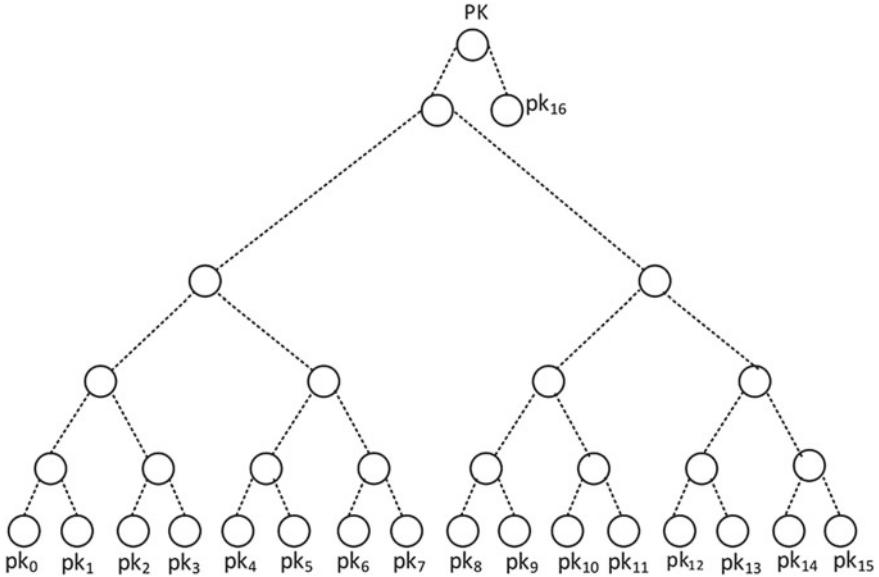


Fig. 4 Key-compression of blockchain-STS

Algorithm 2: Blockchain-STS.keyCompress().

```

Input: [pk0, pk1, ..., pkl-1]
Output: PK
1: define N[(l - 1) * 2 - 1]                                ▷ Declares a perfect binary tree N of height 4
2:  $\sum_{i=0}^{l-2} N[i + 1 - 2] \leftarrow pk_i$                       ▷ Stores pk0 to pk15 in leaf nodes of N
3: define j  $\leftarrow ((l - 1) * 2 - 1)$ 
4: while j > 1 do
5:   define k  $\leftarrow (j/2)$ 
6:   while k < j do                                         ▷ Loop iterates 4 times, and generates an upper level of N in each repetition
7:     N[k/2]  $\leftarrow H(N[k] + N[k + 1])$                          ▷ Computes a new node of N in each of the repetition
8:     k  $\leftarrow k + 2$ 
9:   j  $\leftarrow j/2$ 
10:  PK  $\leftarrow H(N[0] + pk_{l-1})$                                 ▷ Computes compressed pk from root of N and 17th pk-value

```

5 Discussion on Post-quantum Distributed Ledger for IoT

This portion of the chapter explains in detail our introduced Distributed Ledger-STS. The introduced Distributed Ledger includes several activities. An event contains the subsequent information objects: execution time, sensors (Internet-of-Things Informations), docking key(prnkey), digital signatures(σ), and the transaction's successor ID (succID). We will use $trx\ i(n)$ to describe the transaction I data item (0 to 4). SuccID and docking key are both the public keys provided by our intended STS system (Sect. 4). The initial event (i.e., the creation of genesis block) is a succID. The owner creates the event of genesis. Different events receive the ID of their antecedent,

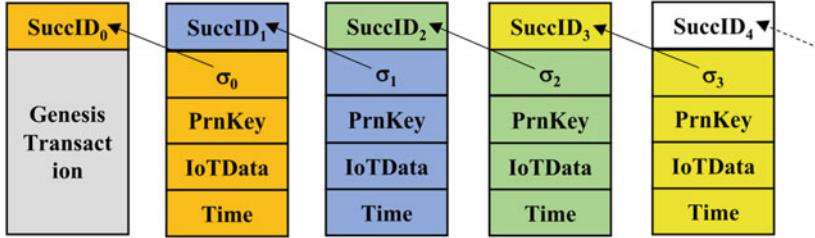


Fig. 5 Transaction structure and chaining

which signifies only a reasonable later agreement of each event keeper before it. When making the genesis block transaction(trx 0), the proprietor generates a public key utilizing our recommended STS scheme (i.e., Blockchain-STS) and save the public key in the genesis block as succID (Algorithm 3). The private key allows trx 0 owners to enable the generation of a new transaction by another node. The event proprietor of the second transaction block(trx 1) must signature the block transaction with a private key that matches the succID in trx 0. The measurement connected peers will be obey trx 1 sign to produce the public key equivalent to the succID collected in trx 0. Similarly, trx 1's succID gave permission to trx 1 owner to give permission to different nodes to create a new event(trx 2); trx 2 keeper has to sign its business utilizing each private key corresponding to the succID collected in trx 1. Figure 5 illustrates transaction structure and chaining, and Algorithm 4 demonstrates how new transactions are created.

Algorithm 3 DL-for-IoT.createGenesis().

Input: ϕ
Output: Genesis Transaction (trx_0)
 1: $trx_0[0] \leftarrow trx_0[1] \leftarrow trx_0[2] \leftarrow trx_0[3] \leftarrow \phi$
 2: $(sk_0, pk_0) \leftarrow DL\text{-OTS}.keyGen()$
 3: $trx_0[4] \leftarrow DL\text{-OTS}.keyCompress(pk_0)$

Algorithm 4 DL-for-IoT.newTransaction().

Input: sk_σ (sk corresponding to $trx_{i-1}[4]$), IoT data
Output: trx_i
 1: $trx_i[0] \leftarrow currentTime$
 2: $trx_i[1] \leftarrow IoT\ data$
 3: $(sk_{prn}, pk_{prn}) \leftarrow DL\text{-OTS}.keyGen()$
 4: $trx_i[2] \leftarrow DL\text{-OTS}.keyCompress(pk_{prn})$
 5: $trx_i[3] \leftarrow DL\text{-OTS}.sign(trx_i[0]+trx_i[1]+trx_i[2], sk_\sigma)$
 6: $(sk_{succ}, pk_{succ}) \leftarrow DL\text{-OTS}.keyGen()$
 7: $trx_i[4] \leftarrow DL\text{-OTS}.keyCompress(pk_{succ})$

5.1 Accepting and Verification of Transaction

This paragraph discusses the rules on transaction confirmation embraced by our suggested DL, namely Blockchain-for-IoT. The companion can attach a new transaction in our proposed model only after the consent of another peer who has confidence and has his or her transactions previously collected in the Blockchain. Several distinct transactions receive their ID from their previous activity, which can only be accomplished after the agreement of the previous transaction holders. Once a peer has

submitted a new transaction, all other partners check the novel activity (each identical algorithm five methods) and subsequently add it to the ledger. Solely trusted peers can store transactions on the ledger in our system model. A colleague with a stake in the directory is trusted (inside each class of a transaction) furthermore may concede a different colleague to supplement a new activity. The new peer is still trusted because the old trustworthy peer has approved it. The season for a wicked companion is insignificant in our suggested model. Furthermore, if a peer has a wicked deed of a remarkable kind, the subsequent peer and his supporter may be excluded by the trusted peers.

Algorithm 5 DL-for-IoT.verifyTransaction().

Input: trx_i
Output: Verified/Failed

- 1: $vk \leftarrow DL\text{-OTS}.\text{verificationKey}(trx_i[0]+trx_i[1]+trx_i[2], trx_i[3])$
- 2: $vkCompressed \leftarrow DL\text{-OTS}.\text{keyCompress}(vk)$
- 3: if $vkCompressed = trx_{i-1}[4]$ then
- 4: Verified
- 5: else
- 6: Failed

5.2 Differentiate Between Trusted and Malicious Peers

This portion of the chapter discusses how our discussed example distinguishes among a trusting plus a hostile companion. A companion that can collect a trade effectively inside the catalog is trustworthy. The transaction proprietor obligation provides the valid signatures of his trade to store a new event in the header (otherwise, the event is unverified and thus rejected). The owner signs his transaction using our suggested “DL- STS” system. The signatures must match an ID previously registered in the record. The transaction previously collected with each identical ID would be the precursor of the current transaction. The owner shall provide the proprietor of that antecedent event with a seed to allow him to sign a new transaction. The seeding from an established owner to the new owner ensures that each current proprietor is a reliable user/companion. Since distinct companions take the identical method to collect the event in the record, all companions deposited their events in the leader are trustworthy. A pair that fails to implement signatures corresponding to a cached ID is marked as a wicked combination, including its action is dismissed.

5.3 Ledger Pruning

The DL-with-IoT offers a higher scalability for the elimination of unnecessary purchases. An owner can delete his transaction until it is no longer necessary. To delete a transaction (say trx_i), trx_i owner must sign it with a private key (prnkey) already registered in trx_i to delete a transaction. Other peers would then validate the signatures and then delete the transaction concerned. For the removal of trx_i , the succID contained in it is easily copied to trx_{i-1} transaction (Algorithm 6). The succID

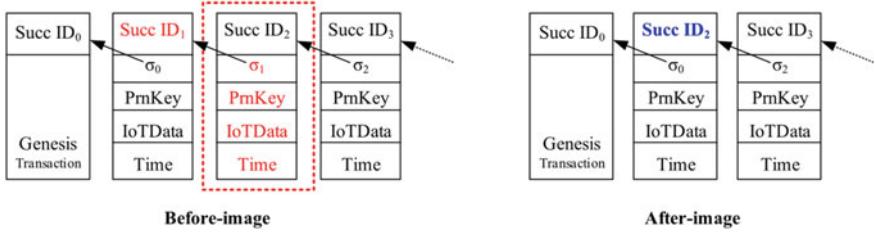


Fig. 6 Ledger-pruning technique

contained in trx_i is essentially the transaction's ID, trx_{i+1} . When this succID is copied to trx_{i-1} , trx_{i+1} will be positioned as trx_i , while the old trx_i will exit the chain (ledger). Figure 6 displays DL photos before and after a transaction has been removed.

Algorithm 6 DL-for-IoT.*removeTransaction()*.

Input: σ_{trx_i} (signatures on transaction to be removed, created using the corresponding sk_{pm})
Output: DL with trx_i removed from it

```

1:  $vk \leftarrow \text{DL-OTS}.\text{verificationKey}(\text{trx}_i, \sigma_{\text{trx}_i})$ 
2:  $vkCompressed \leftarrow \text{DL-OTS}.\text{keyCompress}(vk)$ 
3: if  $vkCompressed = \text{trx}_i[2]$  then
4:    $\text{trx}_{i-1}[4] \leftarrow \text{trx}_i[4]$ 
```

5.4 Working Architecture of Blockchain-for-IoT

Us comprehend some knowledges' architectures [4, 5]. In [5], the planned design includes miners, full nodes (additionally recognized as factors), including Internet-of-Things data nodes. Internet-of-Things sensor nodes create information plus stock information from miners into the box. On behalf of IoT nodes, agents commute with miners. Makhdoom et al. suggested in [4] an interface into which IoT sensor and actuator communicate explicitly with the DL nodes. In this system, both a miner and an agent share a blockchain server and Internet-of-Things nodes interact explicitly with connected peers. Peers are resourceful enough to collect and save sensor information in their blockchain ledger. Due to reasonably small transaction verification and consensus processes, we may exclude an agent's position. Our design assumes that IoT devices do not produce keys, but a connected peer conducts these action in the name of an IoT node community. Peers often retain a DL in order to save information from the related Internet-of-Things sensor [37]. When a part of information is saved in the blocks of blockchain, a peer produces two STS major pairs. Each pair keeps their keys locally. Store a key-pair means just store two SHA384 hash data, private and public key compressed; (each 384-bit). Therefore, the cumulative key size on disc is just 0.097KB. We summarise the following points in our suggested architecture:

1. Two kinds of nodes, IoT nodes and peers are available
2. Data generation of IoT nodes (i.e. sensors)

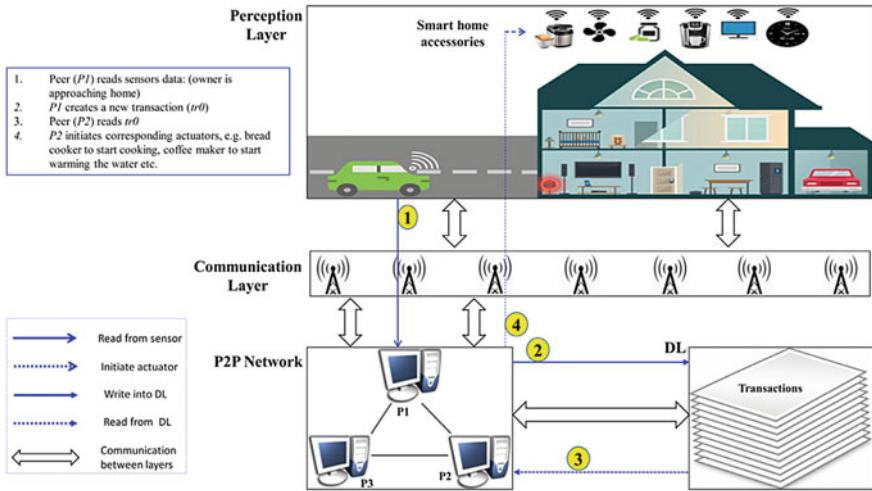


Fig. 7 A smart home architecture incorporating with blockchain-for-IoT

3. A peer has a double role; one is for a number of nodes connected in IoT system, and 2nd is that people keep the Blockchain-DL.
4. Information of IoT system is saved in the distributed ledger by connected peers. A part of information which is generated by a sensor is deposited in the Blockchain-DL by the pair operating as a sensor thing.
5. Peers build and store keys to store data for the sensors
6. Each pair keeps their keys locally

Figure 7 explains the design of our proposed Blockchain-for-IoT in a clever house.

6 Security Analysis for Distributed Ledger STS

For safe execution, Blockchain-STS is a SHA384 hash-based technique that involves a single-way hash feature. In this part, we'll see how the security of Blockchain-STS is based on the single-way of its underlying hash algorithm being reduced. The Blockchain-STS is made up of 4 parts. Key-generation accepts n as a protection variable and gives a key-pair $(\sum_{i=0}^{l-1} (sk_i, pk_i))$. A information-hash (h_m) and a private-key $(\sum_{i=0}^{l-1} sk_i)$ are needed to sign then its return message signature of $m(\sigma^m)$.

Table 3 Key and signature sizes of STS schemes

Scheme	Parameters			Sizes (KB)	
	h_m	n	l_k	key	σ
Lamport	384-bit	384-bit	768	36.9	18.4
WOTS		384-bit	99	4.8	4.8
WOTS ^{PRF}		256-bit	99	3.2	3.2
WOTS ⁺		256-bit	115	3.7	3.2
HORS/PORS		384-bit	65536	3.1MB	1.2
DL-OTS		384-bit	17	0.8	0.8

7 Blockchain-STS Performance Analysis

This segment assesses the neatness and responsiveness of the Blockchain-STS, which is the foundation of our crafted Blockchain-for-IoT. In Sect. 7.1, the main and signature sizes of Blockchain-STS are compared to those of current STS schemes.

7.1 Blockchain-STS Compactness Assessment

Blockchain-STS has the minor key plus sign dimensions of each present single-time signature (STS) system. The primary moreover sign dimensions of Distributed Ledger-STS are compared to those of current typical STS schemes in Table 3. The extent of each information-hash to be signed (h_m), the extent of a natural key/component(n), also this whole quantity of components required to instantiate a scheme all influence the key and signature sizes (w). Those parameters enable the user to change the scheme's assurance level(the security level is determined by the parameters h_m , and n), as well as to create a trade-off between signature value size plus sign production time. To manage nearly 128-bit post-quantum protection, we chose values for h_m , and n . We have also selected the value of parameter w that recommends [11]. Compared to the most common STS system, WOTS, the findings show that Blockchain-STS provides an 84% reduction in both primary and sign dimensions. In addition, Blockchain-STS provides substantial principal and signature size reductions as opposed to other systems.

The original WOTS lightweight versions WOTS + is a standard compact WOTS version that is around 33% smaller than WOTS +. Blockchain-STS is 75% smaller than WOTS +, but Blockchain-STS is 78% smaller than WOTS + when it comes to core dimension.

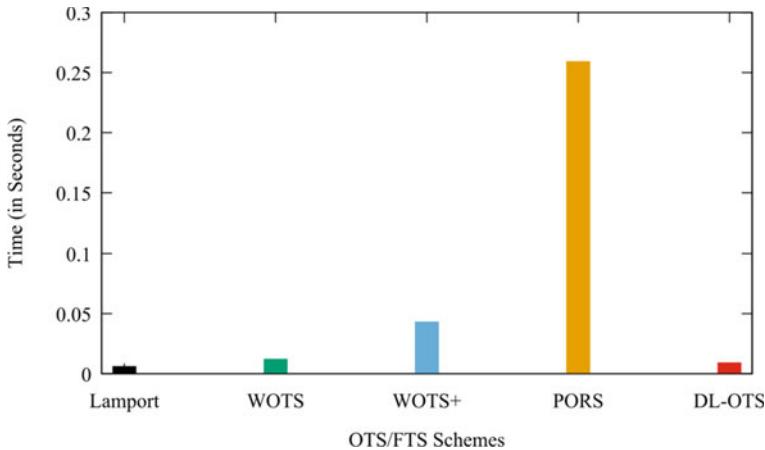


Fig. 8 Key generation time of STS

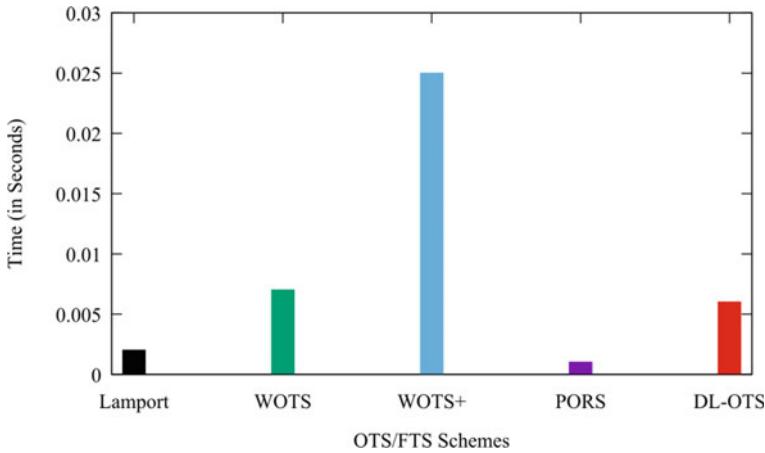


Fig. 9 Signature creation time of STS

7.2 Power and Energy Efficiency of Blockchain STS

This sub-section contrasts the Blockchain-STS implementation period and energy usage to current STS schemes. Distributed Ledger-STS is not just a lightweight but additionally an active and energy-efficient STS system that provides the least time for crucial creation, information signing, signature, and key compression [38]. The charts in Figs. 8, 9, 10 and 11 allow the execution period of Blockchain-STS to be compared with current standard STS systems. Both these systems have been introduced in the “JetBrains PyCharm Community Edition 2018.3.3” environment utilizing the Python language [39]. The findings were obtained from a laptop includ-

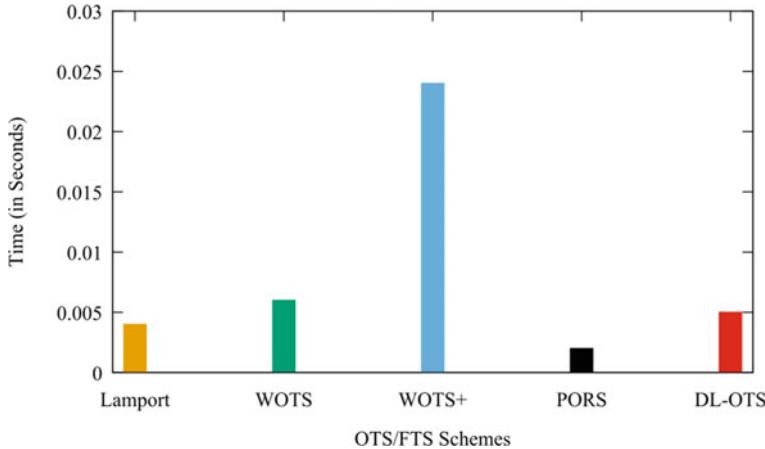


Fig. 10 Signature verification time of STS

ing an Intel Core i3 CPU (2.0 GHz) and 8GBRAM with a 64-bit version of Windows 10. All these findings show that our proposed scheme is effective. The results show that the Distributed Ledger STS production, signature formation, and main compression times are 25%, 14%, and 55% lower than the WOTS scheme. In addition, Blockchain-STS provides 79%, 76%, and 54% reductions in the primary generation, signature creation/verification, and key compression times, sequentially, associated with WOTS+. The graph in Fig. 12 relates Blockchain-STS power usage to other standard STS systems. The findings show that Distributed Ledger STS Blockchain-STS saves 47.9% of energy compared to the popular WOTS system. We also observed the study of Damasevicius et al. in calculating energy consumption [40]. SciPhone i+++ Cell Computer belongs to the testbed of the energy-related tests [41].

8 Conclusion

For IoT-based applications, Blockchain-for-IoT is a fully secured system based on the quantum technology. The Blockchain-for-IoT discussed the problems of combining the two distributing and IoT technologies. Blockchain-for-IoT is characterized by transaction-chaining, book cutting, low-weight agreement. Blockchain-for-IoT is a distributed, quantum-based DL that customizes rules for the transaction chain (as per standard specifications of IoT systems), develops a ledger pruning mechanism, and implements a lightweight consensus mechanism. The Blockchain-for-IoT building block is a new STS system, namely Blockchain-STS. Comparing Blockchain-STS among typical STS schemes, Blockchain-STS is a lightweight, fast, furthermore energy-efficient signature pattern. Compared with the famous Winter-nitz OTS+ schema, Blockchain-STS offers a 75% reduction in signature dimension

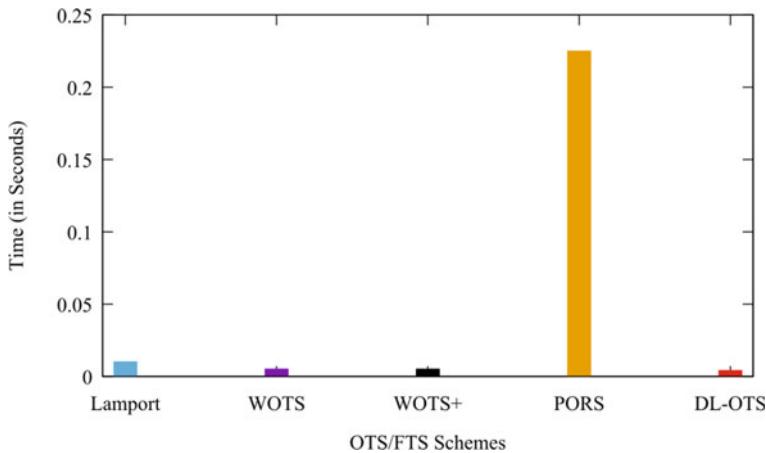


Fig. 11 Key compression time of STS

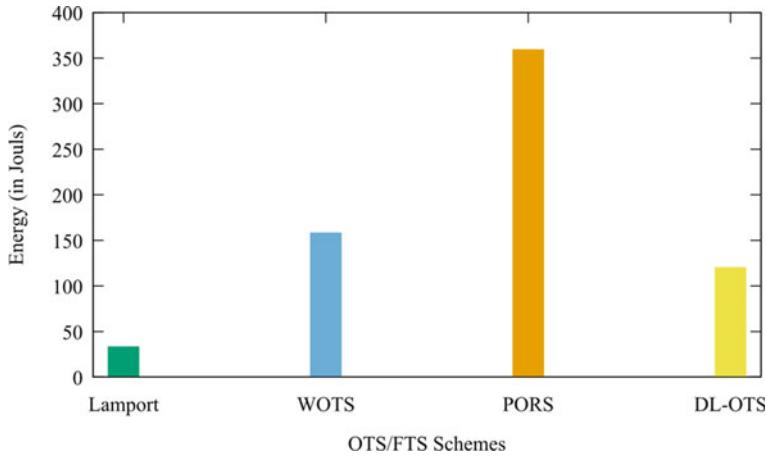


Fig. 12 Energy consumption (in Joules) of STS schemes

and 77% reduction in signature formation period. In addition, Blockchain-STS saves 47.9% more power than Winteritz-OTS +. The suggested Blockchain-for-IoT is a general architecture that can be used after customizing miners for various kinds of IoT utilization (such as smart houses, clever towns, smart grids, or VANETs, etc.). The future study emphasizes the protocols to ensure safe data transfer among IoT nodes and the P2P network. In addition, the proposed architecture can be improved in the future to accommodate complex situations such as complex index modification as several transactions occur or concurrently prune.

References

1. Khan MA, Salah K (2018) IoT security: Review, blockchain solutions, and open challenges. *Futur Gener Comput Syst* 82:395–411
2. Qiu T, Chen N, Li K, Atiquzzaman M, Zhao W (2018) How can heterogeneous internet of things build our future: a survey. *IEEE Commun Surv Tutor* 20(3):2011–2027
3. Roy DG, Mahato B, De D, Buyya R (2018) Application-aware end-to-end delay and message loss estimation in internet of things (iot)-mqqt-sn protocols. *Futur Gener Comput Syst* 89:300–316
4. Makhdoom I, Abolhasan M, Abbas H, Ni W (2019) Blockchain's adoption in iot: the challenges, and a way forward. *J Netw Comput Appl* 125:251–279
5. Qureshi KN, Din S, Jeon G, Piccialli F (2020) Link quality and energy utilization based preferable next hop selection routing for wireless body area networks. *Comput Commun* 149:382–392
6. Cheng C, Lu R, Petzoldt A, Takagi T (2017) Securing the internet of things in a quantum world. *IEEE Commun Mag* 55(2):116–120
7. Yu Y, Li Y, Tian J, Liu J (2018) Blockchain-based solutions to security and privacy issues in the internet of things. *IEEE Wirel Commun* 25(6):12–18
8. Wu X, Jiang G, Wang X, Xie P, Li X (2019) A multi-level-denoising autoencoder approach for wind turbine fault detection. *IEEE Access* 7:59376–59387
9. Chaudhary R, Jindal A, Aujla GS, Kumar N, Das AK, Saxena N (2018) Lscsh: lattice-based secure cryptosystem for smart healthcare in smart cities environment. *IEEE Commun Mag* 56(4):24–32
10. Bernstein DJ, Hopwood D, Hülsing A, Lange T, Niederhagen R, Papachristodoulou L, Schneider M, Schwabe P, Wilcox-O'Hearn Z (2015) Sphincs: practical stateless hash-based signatures. In: Annual international conference on the theory and applications of cryptographic techniques. Springer (2015), pp 368–397
11. Hülsing A (2013) Wots+—shorter signatures for hash-based signature schemes. In: International conference on cryptology in Africa. Springer (2013), pp 173–188
12. Roy DG, Das P, De D, Buyya R (2019) Qos-aware secure transaction framework for internet of things using blockchain mechanism. *J Netw Comput Appl* 144:59–78
13. Liu Y, Wang K, Lin Y, Xu W (2019) A lightweight blockchain system for industrial internet of things. *IEEE Trans Industr Inf* 15(6):3571–3581
14. Aggarwal D, Brennen GK, Lee T, Santha M, Tomamichel M (2017) Quantum attacks on bitcoin, and how to protect against them, arXiv preprint [arXiv:1710.10377](https://arxiv.org/abs/1710.10377)
15. Costello C, Jao D, Longa P, Naehrig M, Renes J, Urbanik D (2017) Efficient compression of sidh public keys. In: Annual international conference on the theory and applications of cryptographic techniques. Springer, pp 679–706
16. Reyna A, Martín C, Chen J, Soler E, Díaz M (2018) On blockchain and its integration with iot. challenges and opportunities. *Future Gener Comput Syst* 88:173–190
17. Din S, Paul A, Ahmad A, Gupta BB, Rho S (2018) Service orchestration of optimizing continuous features in industrial surveillance using big data based fog-enabled internet of things. *IEEE Access* 6:21582–21591
18. Roy DG, De D, Alam MM, Chattopadhyay S (2016) Multi-cloud scenario based qos enhancing virtual resource brokering. In: 2016 3rd international conference on recent advances in information technology (RAIT). IEEE, pp 576–581
19. Underwood S (2016) Blockchain beyond bitcoin. *Commun ACM* 59(11):15–17
20. Novo O (2018) Blockchain meets iot: an architecture for scalable access management in iot. *IEEE Internet Things J* 5(2):1184–1195
21. Zhang Y, Wen J (2017) Peer-to-peer network application, vol 10, p 983
22. Shrestha R, Bajracharya R, Shrestha AP, Nam SY (2020) A new type of blockchain for secure message exchange in Vanet. *Digital Commun Netw* 6(2):177–186
23. Winter E, Forshaw S, Ferrario MA (2018) Measuring human values in software engineering. In: Proceedings of the 12th ACM/IEEE international symposium on empirical software engineering and measurement, pp 1–4

24. Roy DG, Mahato B, Ghosh A, De D (2019) Service aware resource management into cloudlets for data offloading towards iot. *Microsyst Technol*, 1–15
25. Jiang H, Zhang Z, Ma Z (2019) Tighter security proofs for generic key encapsulation mechanism in the quantum random oracle model. In: International conference on post-quantum cryptography. Springer, pp 227–248
26. Lee B, Lee J-H (2017) Blockchain-based secure firmware update for embedded devices in an internet of things environment. *J Supercomput* 73(3):1152–1167
27. Güneysu T, Oder T (2017) Towards lightweight identity-based encryption for the post-quantum-secure internet of things. In: 18th international symposium on quality electronic design (ISQED). IEEE, pp 319–324
28. Fernandez-Carames TM, Fraga-Lamas P (2019) A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. *IEEE Access* 7:45201–45218
29. Smart NP (2018) Topics in cryptology—CT-RSA 2018: the cryptographers' track at the RSA conference 2018, San Francisco, April 16–20, 2018, Proceedings, vol 10808. Springer (2018)
30. Din S, Ahmad A, Paul A, Rho S (2018) Mgr: Multi-parameter green reliable communication for internet of things in 5g network. *J Parallel Distrib Comput* 118:34–45
31. Mahato B, Roy DG, De D (2021) Distributed bandwidth selection approach for cooperative peer to peer multi-cloud platform. *Peer-to-Peer Netw Appl* 14(1):177–201
32. Gohar M, Ahmed SH, Khan M, Guizani N, Ahmed A, Rahman AU (2018) A big data analytics architecture for the internet of small things. *IEEE Commun Mag* 56(2):128–133
33. Ahmad A, Khan M, Paul A, Din S, Rathore MM, Jeon G, Choi GS (2018) Toward modeling and optimization of features selection in big data based social internet of things. *Futur Gener Comput Syst* 82:715–726
34. Liu Z, Pöppelmann T, Oder T, Seo H, Roy SS, Güneysu T, Großschädl J, Kim H, Verbauwhede I (2017) High-performance ideal lattice-based cryptography on 8-bit avr microcontrollers. *ACM Trans Embed Comput Syst (TECS)* 16(4):1–24
35. Roy DG, Mahato B, De D (2019) A competitive hedonic consumption estimation for iot service distribution. In: URSI Asia-Pacific radio science conference (AP-RASC). IEEE, pp 1–4
36. Guha Roy D, Srirama SN (2021) A blockchain-based cyber attack detection scheme for decentralized internet of things using software-defined network. In: Software: practice and experience
37. Roy DG, Das M, De D (2018) Cohort assembly: a load balancing grouping approach for traditional wi-fi infrastructure using edge cloud. In: Methodologies and application issues of contemporary computing framework. Springer, pp 93–108
38. Pöppelmann T, Güneysu T (2014) Area optimization of lightweight lattice-based encryption on reconfigurable hardware. In: IEEE international symposium on circuits and systems (ISCAS). IEEE, pp 2796–2799
39. Hernández-Rojas DL, Fernández-Caramés TM, Fraga-Lamas P, Escudero CJ (2018) Design and practical evaluation of a family of lightweight protocols for heterogeneous sensing through ble beacons in iot telemetry applications. *Sensors* 18(1):57
40. Damaševičius R, Ziberkas G, Štuikys V, Toldinės J (2012) Energy consumption of hash functions. *Elektronika ir elektrotechnika* 18(10):81–84
41. Roy DG, Ghosh A, Mahato B, De D (2018) Qos-aware task offloading using self-organized distributed cloudlet for mobile cloud computing. In: International conference on computational intelligence, communications, and business analytics. Springer, pp 410–424

BCoT: Concluding Remarks



Siddhartha Bhattacharyya, Partha Sarathi Banerjee, Amiya Karmakar,
Debashis De, and Joel J. P. C. Rodrigues

Abstract The advent of cloud computing has ensured a fertile soil for efficiently handling distributed computing. However, it calls for the provisioning of high-configuration infrastructure, including advanced servers and high-bandwidth networks for augmenting storage and computation-intensive services. To address this problem, IoT services have envisaged a centralized cloud-enabled IoT framework modeled as a black box facilitating resilience, adaptability, reliability, trust, confidentiality, and integrity, reducing maintenance costs, and enabling time-efficient IoT application support. Blockchain technology stands out to be one of the most suitable candidates for enabling a secure and distributed IoT ecosystem, thereby adding a helping hand in countering these inherent challenges and issues. Blockchain technology is a conglomerate of cryptography, public key infrastructure, and economic modeling to induce distributed database synchronization in peer-to-peer networking supported by a decentralized consensus. The underlying features of decentralized architecture, immutability, verifiability, and fault-resistance make it suitable for envisaging a properly coordinated and distributed IoT environment, giving rise to a Blockchain for Internet of Things (BCoT).

S. Bhattacharyya (✉)
Rajnagar Mahavidyalaya, Rajnagar,
West Bengal, India

P. S. Banerjee
Department of Information Technology, Kalyani Government Engineering College, Kalyani, West Bengal, India

A. Karmakar · D. De
Department Computer Science and Engineering, Centre of Mobile Cloud Computing,
Maulana Abul Kalam Azad University of Technology, Kolkata, West Bengal, India

J. J. P. C. Rodrigues
College of Computer Science and Technology, China University of Petroleum (East China),
Qingdao 266555, China

Senac Faculty of Ceará, Fortaleza-CE, Brazil
Covilhã Delegation, Instituto de Telecomunicações, Covilhã, Portugal

Keywords Blockchain · Internet of Things (IoT) · BCoT · Industry 4.0

1 Introduction

Prolific digitization associated with the advent of the Internet of Things (IoT) has revolutionized a paradigm shift in the industrial and manufacturing sector coined by the term “Internet of Things (IoT)”. The Industry 4.0 standard incorporates the power of smart technology, real-time data analysis and smart infrastructures, cyber-physical systems, and intelligent cognitive computing in a cloud environment to analyze the explosion in data produced and consumed. IoT promotes multi-disciplinary business intelligence and supports well-organized quality management and perceptible supply chains coupled with prognostic maintenance, improved field services, asset tracking, and imperishable green practices. As such, an IoT ecosystem is meant for effective control of numerous physical and virtual smart devices interconnected together and distributed across the entire physical world to enable collection and secured exchange and analysis of the massive amount of ambient data. The advent of cloud computing has provided a wide range of possibilities for efficiently handling distributed computing. However, it calls for the provisioning of high-configuration servers and high-speed networks for augmenting storage and computation-intensive services. In order to address this problem, IoT services have envisaged a centralized cloud-enabled IoT framework modeled as a black box facilitating the emergence of a resilient, adaptable, fault-tolerant, trusted, and secure service architecture that leverages reduced maintenance costs and time-critical application support. Blockchain technology stands out to be one of the most suitable candidates for enabling a secure and distributed IoT ecosystem, thereby adding a helping hand in countering these inherent challenges and issues. Blockchain technology is a conglomerate of cryptography, public key infrastructure, and economic modeling to induce distributed database synchronization in peer-to-peer networking supported by a decentralized consensus. The underlying features of distributed architecture, immutability, verifiability, and fault-resilience make it suitable for envisaging a decentralized IoT infrastructure, thereby giving rise to a Blockchain for Internet of Things (BCoT) [1–5]. Different industry-based solutions and platforms including Lola [6], COSMOS [7], Dajie [8], Filament [9], Slock.it [10], Smart Axiom [11], BlockVerify [12], Xage Security [13], Ubirch [14], Multichain [15], ShoCard [16], Chronicled [17], Uniquid [18], Riddle and Code [19], Datum [20] have been introduced to cater public, private, and federated blockchains with the goal of addressing confidentiality and integrity, monetization, reliability, trust, identity, and data management issues. However, numerous operational and technical challenges are to be conquered to achieve an absolute IIoT decentralization using blockchain due to the wide spectrum of the IoT applications including the food industry, e-voting, real estate, cyber-security, healthcare services, supply chain and logistics, music, insurance, energy and smart grid management, and apparel industry, to name a few. Apart from the technical challenges out of processing, storage, communications, and availability, associated

risks, and regulatory issues also pose serious challenges. Issues of security, privacy, trust, and scalability also remain matters of serious concern in this regard.

This chapter attempts to highlight the accompanying challenges and issues in a BCoT architecture while putting forward the recent best practices that have evolved to counter these issues.

2 Key Takeaways

This volume is focused on targeting these glaring issues with due recourse to the challenges encountered in having a full-fledged BCoT in practice while stressing different novel initiatives to address the concerns. The volume is thus aimed to foster a knowledge-base on blockchain technology highlighting the framework basics, operating principles, and different incarnations. The fundamental problems encountered in existing blockchain architectures and means for removing those have been covered. It also touches upon blockchain-based IoT systems and applications. The book also covers the applications and use cases of blockchain technology for industrial IoT systems. In addition, methods for inducing computational intelligence into existing blockchain frameworks, thereby thwarting most limitations, are also on the cards.

Blockchain in IoT has been duly emphasized with reference to a detailed overview on IoT and industrial IoT (IIoT) including the proof of concepts of distributed ledger technology (DLT). The issues of identity management interoperability in IoT and IIoT have been addressed with a case study of the Polkadot protocol with relay chain. In addition, Hyper Ledger Indy also been discussed with examples of onboard processing of drones. This exhaustive treatment on the subject matter has reiterated the effective use of blockchain in IoT for identity management.

The irresistible explosion in the volume of data in the virtual world has opened the need for the concept of cloud computing. As a fallout, data security, confidentiality, integrity, and availability on-demand have assumed paramount importance. Traditional solutions such as cryptography only are no longer effective enough. Recent trends in hybrid frameworks of data encryption algorithms like the Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) have been evolved for the effective distribution of keys to thwart potential attacks in the SaaS layer. Furthermore, authentication using a decentralized block-chain architecture can ensure data availability and integrity in the cloud IaaS layer, thereby adding to cloud security (CIA).

A balanced combination of blockchain, the Internet of Things, and artificial intelligence is expected to boost business models, goods, and services. Machine learning algorithms can help make blockchain-based IoT network smart applications that are more robust to attacks.

Blockchain technology has also made inroads into the financial sector indispensable in data management and transparent money transfer. The integration of blockchain technology into the banking domain is inevitable, and the policymakers are busy with their persistent endeavor to make this integration seamless with proper

checks and balances. Regarding handling possible risks associated therein, promising fintech companies in technical collaboration with blockchain technology specialists are already taking this new paradigm one step ahead with several chatbot-managed branches, chatbot financial advisory services, and asset management applications. The use of blockchain technology for streamlining the process for digital identity, cross-border payments, KYC updates, and credit rating evinces the relevance of the technology along with IoT. The integration of servers, providing accessibility on a real-time basis, and multiple device-based operations of accounts have made banking very simple, cost-effective, and popular.

The most abstract perspective of blockchain-enhanced identity management for IoT is the IAM models designed from a techno-political point of view. It specifies not only the methodology for the identification of an entity in an IoT environment but also indicates the ways with which the system can interact with other entities. Adaptive integration of IAM contributes to the model abstraction by precise scaling and interaction with the IoT-based system. At the same time, digital identity is also evolving due to the significance of its use both in any IT implementation and in users' everyday life. Its uses find applications in a wide spectrum of scenarios ranging from the simplest communication between a smartphone and a light bulb to identifying a digital twin in any environment. The SSI model is considered the last stage of the digital identity evolution, which can be owned and managed by entities themselves. The application adaptive combination of the technologies mentioned above poses a large scope of research challenges for the designers. Performance in terms of speed and data consumption is a matter of concern, especially for low-end devices operating on the edge. IoT systems are characterized by extremely fast response time with lightweight architecture. Executing computation-intensive cryptographic algorithms like ZKP is a costly task for edge nodes in terms of both time and storage. A blockchain-enhanced IAM system adapted to IoT environments is to offer truly decentralized digital IAM. At the same time, every device and user can verify and be verified across an IoT network in real-time environments.

Blockchain-enabled IIoT networks are evolving at a very high pace. It is becoming a new standard in worldwide progress. The combination of blockchain and IIoT will bring huge technological leaps that will bring remarkable enhancements to various facets of human life to make our society smarter and easier. Recent models efficiently utilize the computational power of the devices in the IIoT network to create a blockchain using the most suitably fitting hash algorithm. New benchmarking algorithms can be designed to be applicable on wide-ranging devices instead of computationally similar devices. These benchmarking algorithms also help to cluster the numerous devices in the IIoT network into different tiers. Based on the tier of a device, a computationally suitable hash algorithm can then be devised. Securing industrial IoT using efficient blockchain design enhances and expands IIoT applications.

With the advent of the quantum computing paradigm, blockchain-for-IoT has become a fully secured system. Quantum-based blockchain-for-IoT is a distributed, quantum-based DL that customizes rules for the transaction chain (as per standard specifications of IoT systems), develops a ledger-pruning mechanism, and implements a lightweight consensus mechanism. The building block is a new single-time

signature system, viz., the blockchain-STS. Compared to the typical STS schemes, blockchain-STS is a lightweight, fast and energy-efficient signature pattern.

The readers would benefit from the rich technical content in this rapidly emerging field, thereby enabling a skilled workforce for the future.

References

1. Ali MS, Vecchio M, Pincheira M, Dolci K, Antonelli F, Rehmani MH (2018) Applications of blockchains in the internet of things: a comprehensive survey. *IEEE Commun Surv Tutor* 1–42. <https://doi.org/10.1109/COMST.2018.2886932>
2. Miraz MH (2020) Blockchain of things (BCoT): the fusion of blockchain and IoT technologies. In: Advanced applications of blockchain technology, pp 141–159. Springer, Singapore
3. Conoscenti M, Vetro A, De Martin JC (2016) Blockchain for the internet of things: a systematic literature review. In: 2016 IEEE/ACS 13th international conference of computer systems and applications (AICCSA), pp 1–6
4. Reyna A, Martin C, Chen J, Soler E, Daz M (2018) On Blockchain and its integration with IoT. Challenges and opportunities. *Futur Gener Comput Syst* 88:173–190
5. Fernández-Caramés TM, Fraga-Lamas P (2018) A review on the use of blockchain for the internet of things. *IEEE Access* 6:32979–33001
6. Lola ICT, blockchain enables citizens to manage own identity data. <https://lola-ict.org/news/2018/12/17/blockchain-enables-citizens-to-manage-own-identity-data>. Last Accessed 5 Oct 2021
7. Interchain foundation, internet of blockchains. <https://cosmos.network/>. Last Accessed 30 Sept 2021
8. Crunchbase Inc., DAJIE Ltd. <https://www.crunchbase.com/organization/dajie-ltd>. Last Accessed 30 Sept 2021
9. Crunchbase Inc., Filament. <https://www.linkedin.com/company/filament-networks/>. Last Accessed 1 Oct 2021
10. Crunchbase Inc., Slock.it. <https://www.crunchbase.com/organization/slock-it>. Last Accessed 1 Oct 2021
11. Smartaxiom, building a smarter and safer world. <https://www.smartaxiom.com/>. Last Accessed 31 Aug 2021
12. Crunchbase Inc., blockverify. <https://www.crunchbase.com/organization/blockverify>. Last Accessed 27 Sept 2021
13. Xage Security Inc., zero trust security for the real world. <https://xage.com/>. Last Accessed 27 Sept 2021
14. Ubirch cyber security LLC, blockchain. <https://ubirch.com/de/>. Last Accessed 30 Sept 2021
15. Coin Sciences Ltd., “Enterprise blockchain. That Actually Works”, Accessed September 27, 2021, <https://www.multichain.com/>
16. PingIdentity, it’s your identity. Own it. <https://www.shocard.com/en.html>. Last Accessed 5 Oct 2021
17. Chronicled, trust & automation between companies. <https://www.chronicled.com/>. Last Accessed 5 Oct 2021
18. UNIQUID, connect and control IoT devices at scale. <https://uniquid.com/>. Last Accessed 5 Oct 2021
19. RIDDLE&CODE, “Riddle & Code”. <https://www.riddleandcode.com/>. Last Accessed 5 Oct 2021
20. Datum, blockchain data storage and monetization. <https://datum.org/>. Last Accessed 1 Oct 2021

Index

A

Abstraction, 29
Access control system, 270
Access Control Mechanism (ACM), 216
Access management, 209–211, 213, 214, 216
Accuracy, 175, 178
Active Usecases, 130
Advanced Encryption Standard (AES), 154, 156, 166
Advantages of Private Blockchain, 32
Advantages of Public Blockchain, 30
Anonymity, 49, 213
Application Program Interface (API), 89, 182
Architecture, 4, 6–14, 140, 141, 152
Architecture of IoT system, 268
ArcTouch, 73
Artificial Intelligence, 173
Asymmetric, 225, 230
Atomic CPS, 84
Attack, 146, 147, 149
Attributes, 212, 215, 219
Authentication, 145, 149, 217, 223, 229
Authorization, 212, 217, 218, 223, 230, 232, 234
Automotive insurance, 187
Availability, 144, 149, 167

B

Backup, 145, 149
Banking frauds, 199
Benchmarking algorithm, 244, 249, 263
Benchmark score, 244

Benefits

blockchain, 28
Bitcoin, 24, 49, 240, 241, 261, 262
Block, 51
Blockchain (BC), 1–3, 11–16, 50, 81, 114, 152, 155, 166, 181–184, 186, 188–197, 199, 202–205, 268
Blockchain and Interoperability, 131
Blockchain based application, 271
Blockchain based architecture, 272
Blockchain miner, 281
Blockchain Network, 212, 213, 225, 227, 231
Blockchain of Things (BCoT), 1, 3, 14–16
Blockchain Technology, 171, 172
Blockchain Terminals (BCTs), 91

C

Capital market transactions opportunities, 33
Central Know Your Customer (CKYC), 190
Certificate Authority (CA), 98, 230–232
Chronicled, 72
Classification, 171
Clearing and Settlement systems, 195
Cloud computing, 141, 145, 173
Cloud Security (CIA), 142–144
Cloud Service Provider, 141, 156, 166
Cloud storage, 149, 155, 268
Cluster, 237, 263
Communication medium, 273
Communication Technology (ICT), 82
Compactness assessment of STS, 283
Complexity, 244, 249

- Computational power, 238, 243, 244, 246, 247, 249, 251, 253, 254, 260, 261, 263
- Conclusion, 167
- Confidentiality, 143, 146, 166
- Confusion matrix, 175
- Connected banking, 181, 184, 185
- Consensus, 2, 4, 11, 16, 153, 158, 212, 213, 227, 239, 241, 244, 247, 251, 252, 254
- Consortium Blockchain, 32
- Constrain Applications Protocol (CoAP), 101
- Control framework, 99
- Convergence, 239, 243
- Cyber-Physical System (CPS), 82
- Credentials, 127, 212
- Credit reporting, 197
- Cross-border transfers opportunities, 34
- Crypto agility, 243, 244
- Cryptocurrency, 27, 270
- Cryptographic, 24, 209, 210, 213, 219, 220, 222–225, 230
- Cryptographic hash, 242, 243, 262
- Cryptography, 151, 154, 166, 210, 212, 213, 224, 240, 242, 254, 274
- Customer credit offering, 182
- Cyber-Physical System (CPS), 82
- D**
- Data
- blockchain, 25
 - DATA-COIN, 63
 - Data layer, 11
 - Data protection, 268
 - Data security, 149, 155, 166
 - Data violations, 146, 150
 - DDoS attacks, 104
 - Decentralization, 28, 52 challenges, 39
 - Decentralized, 2, 4, 15, 142, 152, 167, 210, 214, 218, 219, 221, 224, 225, 228, 230, 231 ledger, 27
 - Decentralized Finance, 210
 - Decentralized Identifiers (DIDs), 119, 218, 220, 221, 222, 232, 233
 - Decentralized Identities, 218
 - Decentralized Public Key Infrastructure (DPKI), 210, 225, 230–232
 - Decryption, 151, 158, 161
- Detection rate, 175
- Device management, 270
- Dew, 1, 8, 10, 13, 14
- DIAM-IoT, 223, 233
- Digital ecosystem, 182, 185
- Digitized banking, 184, 186
- Disadvantages of Private Blockchain, 32
- Disadvantages of Public Blockchain, 31
- Distributed, 152, 166, 239–241, 263
- Distributed Control System (DCS), 96
- Distributed directory, 272
- Distributed ledgers, 3, 188, 267
- Distributed Ledger Technologies, 212, 222, 223
- Distributed time-based consensus, 241
- Drones, 128
- Dynamic framework, 83
- Dynamic physical processes, 83
- E**
- Ecosystem, 43
- Edge, 7, 8, 10
- Efficiency, 2, 8
- Electronic Medical Record (EMR), 94
- Electronic Welfare Records (EHRs), 94
- Elliptic Curve Cryptography (ECC), 151, 162, 166
- Embedded sensors, 273
- Emercoin, 231
- Emerging trends in IoT, 271
- Encryption, 2, 151, 157
- Energy efficiency of STS, 284
- Energy Consumption challenges, 39
- Environment component, 84
- Ethereum, 58, 227, 229, 231, 232
- Ethereum and Bitcoin, 132
- Execution time, 161
- F**
- False negative, 176
- False positive, 176
- False Positive Rate, 176
- Federated Identity (FId), 217
- Fiber, 73
- 51% attack, 16
- Financial Services, 34
- Fine-grained access control, 117
- Firmware, 270
- Fog, 8, 9, 13
- Fog computing, 102
- Frameworks of Frameworks (CPSoS), 86

Fraud, 181, 182, 184, 187, 190, 197–199,
203
FX trading
opportunities, 34

G

GAFA, 182
Ganache, 15
Gateway, 11, 12
Genesis block, 240, 278
Global digital payment methods, 182
Governance, 211, 213
Grid+, 74

H

Hackers, 144, 149, 156
Hardware, 2, 9, 13
Hash, 4, 11, 25
Hashing, 152, 157, 166, 270
Hashing Algorithms, 224
Hdac, 62
Health insurance, 187, 188
Healthcare, 6, 8, 12, 94
opportunities, 35
Health Insurance Portability and
Accountability Act (HIPAA), 94
Helium, 72
Heterogeneity, 2, 9
Hierarchy, 212–214
Home insurance, 187, 188
Human Machine Interface (HMI), 96
Hybrid blockchain, 33
Hyperledger, 58
Hyperledger Indy, 122
HYPR, 74

I

IaaS, 146, 150
IAM, 210–219, 222–225
IAM models, 210, 212, 233
Identification, 210, 213, 214, 229
Identifier, 212
Identity, 209–214, 216–225, 227, 229, 230,
232–234
Identity Management
opportunities, 36
Identity Provider (IdP), 212, 213, 219
Image problem, 40
Immutability, 29, 53
Immutable, 35, 237, 238, 240, 242
Immutable ledger, 270

Impression attacks, 102
Improved K-Nearest Neighbor, 171, 174
Incumbent parties, 43
Industrial computing, 84
Industrial Control Systems (ICS), 95, 96
Industrial IoT (IIoT), 81, 114
Industry 5.0, 1, 2
Instant Karma PKI (IKP), 232
Insurance Sector
opportunities, 36
Integrity, 144, 150, 166
Intelligent transportation (ITS), 98
Internet of Things (IoT), 1–3, 5–16, 23, 48,
82, 90, 114, 140, 155, 172, 174, 181
Internet-of-Vehicles (IoV), 98
Interoperability, 68
challenges, 40
IOTA, 59, 270
IOTEX, 270
IoT nodes, 281
Issuer, 218, 220

K

Key compression, 277
Key generation, 274

L

Lack of awareness, 41
Lack of cooperation, 41
Lack of Regulatory Clarity, 40
Lack of Standardization, 40
Lack of Talent, 41
Large physical frameworks, 86
Latency, 241–243, 262
Ledger, 212, 213, 225, 231, 240, 241
Ledger pruning, 280
Life insurance, 187, 188
LightChain, 241, 270
Lightweight, 11, 13, 15, 16
Light-weight consensus, 269
Lightweight scalable blockchain, 241
Limitations, 16
Logic Controllers (PLC), 95

M

Machine learning, 171, 173, 174
Malicious peer, 280
Management hub, 12, 13
Merkle hash tree, 277
Merkle tree, 4, 5

Messages Queues Telemetry Transports (MQTTs), 101
 Metamask, 15
 Methodology, 156
 Miners, 28
 Minors, 52
 Mobile, 6
 Mobile banking, 182, 184, 187, 196
 Modification, 144, 150, 153
 Monitoring of consortium accounts opportunities, 34
 Motivations, 239
 Multi-Model Modeling (MPM), 84
 Multi-tenancy, 146, 147
 Music Industry opportunities, 37

N
 Namecoin, 231
 Name/Value Storage (NVS), 231
 Near-Field Communication (NFC), 7
 NetObjex, 73
 Network, 2–4, 6–8, 13–16
 Network attack, 171
 Networking systems, 83
 Nodes, 2, 4, 6–8, 11, 13, 16, 126
 Nonce, 240, 251
 Non-repudiation, 145, 151

O
 One-Click Dapp, 15
 Opportunities for Blockchain, 33
 Organizational Challenges, 41
 Ouroboros, 242

P
 P2P, 91
 P2P network, 271
 PaaS, 141, 146, 150
 Pairwise Unique Identifiers, 124
 Parachain, 133
 Pay later, 182
 Peer-to-peer, 27
 Performance, 148, 154, 159
 Performance analysis of STS, 283
 Personalized banking, 186
 Physical component, 84
 Physical Electronics, 84
 PKIs, 105, 225, 230, 231
 Point of Sales, 35
 Polkadot, 132

Post-quantum distributed ledger, 278
 Pretty Good Privacy (PGP), 223
 Previous block blockchain, 25
 Privacy, 2, 15, 16, 142, 146, 209–211, 213, 214, 217, 221–224, 228–230
 Privacy preserving, 114
 Privacy vulnerability, 11
 Private blockchain, 31
 Private key, 274
 Process of creating encrypted KYC, 192
 Processor, 243, 244, 247, 249, 261
 Produce gigabytes (GB), 100
 Productivity paradox, 41
 Proof, 220, 222–225, 230
 Proof-of-Property, 241
 Proof-of-Stakes (PoSs), 67, 104
 Proof-of-Works (PoWs), 27, 49, 66, 104, 225, 227, 251, 269
 Protection, 143, 146, 147, 155
 Prover, 225, 226
 Pseudo-namelessness, 65
 Pseudonymity, 42, 71
 Public Blockchain, 30
 Public key, 274
 Public-Key Infrastructure (PKI), 98, 105
 Python3, 253, 254

Q
 Quality of Services (QoS), 92
 Quantum computer, 269
 Quantum Computing, 16
 Quantum digital signature, 267

R
 Real Estate opportunities, 38
 Redundancy, 144, 155
 Redundant Byzantine Fault Tolerance (RBFT), 126
 Reliability, 145
 Remix, 14
 Re-play attacks, 102
 Reputation, 71
 Retail banking, 184, 185, 199
 Revocation of Entry, 130
 Roles, 212, 213
 RSA, 151, 157, 161
 Running Nodes, 135

S

- Scalability, 2, 15, 42, 67
- Secure Banking, 184, 187
- Secure Hash Algorithm (SHA), 152, 166
- Security analysis of STS, 282
- Security and Privacy, 42
- Security Issues, 140, 145, 150
- Security Messages (BSMs), 98
- Security risks, 141, 145
- Selection, 241, 243, 252, 253
- Selfish mining, 16
- Self-Sovereign Identity (SSI), 122, 220, 221, 234
- Sensor, 1, 6, 8, 11
- SHA384, 274
- SiD, 13
- Signature creation, 275
- Signatures, 223, 230
- Simulated plant, 253, 254
- Single time signature, 267
- Single Point of Failure (SPF), 213
- Smart, 6
- Smart application, 174, 175
- Smart contract, 3, 13, 14, 134, 219, 220, 225, 231
- Smart Grid, 99
- Software-as-a-Service (SaaS), 150, 156, 166
- Steps in developing a smart contract, 189
- Steps in Letter of Credit
 - IoT enabled Trade finance, 194
 - manual procedure, 193
- Steps in using UID, 192
- Stewards, 123
- Stock Market Dealing, 33
- Streamr, 63
- Structure
 - blockchain, 26
- STS scheme, 274
- Summary, 43
- Supply Chain
 - opportunities, 38
- Sybil attacks, 102
- Syndicate lending, 181, 190
- Synergistic multiple proofs, 270
- System of Systems (SoS), 86, 87

T

- Tangle, 270
- Technical Challenges, 42
- Technologies, 3, 4, 7, 8, 11
- Tier I, 244, 254, 256, 260

Tier II, 254, 256, 260

- Tier III, 254, 256, 260**
- Tier IV, 244, 256, 260**
- Timestamped, 24
- Token, 244, 246, 249, 251
- Trade finance, 186, 190, 193, 194
 - opportunities, 34
- Traditional K-Nearest Neighbor, 171, 175
- Traditional system, 140
- Transaction, 4, 11, 15
- Transaction Speed, 135
- Transparency, 29
- Transport-Layer Security (TLS1.2), 101
- True negative, 176
- True positive, 176
- Truffle, 15
- Trust Actor, 123
- Trustless, 2
- Trustworthy peer, 280

U

- Unauthorized access, 210

V

- Validator, 218, 220
- VANET, 270
- VCs, 221–224, 229, 232, 233
- VeChain, 62
- Vehicle to Infrastructure (V2I), 98
- Vehicle to Vehicle (V2V), 98
- Verification of signature, 277
- Verification of transaction, 279
- Verifier, 225, 226
- Verinym, Pseudonym, 124
- Voting
 - opportunities, 39
- Vulnerabilities, 237, 238, 244, 246
- Vulnerable, 11, 16, 144, 164

W

- Wallet, 125
- Wallets, 220, 223–225
- Walton-chain, 62
- Web of Things (WoT), 91
- Wintermute-OTS+, 271

X

- X.509, 223, 230, 232
- Xage, 74

- Z**
Zcash, 228
Zerocoin, 228
Zero-Knowledge, 210, 225, 230
Zero Knowledge Proof (ZKP), 118, 210,
 224–229
Zk-PoL, 229
ZK-SNARKs, 228