Performance Analysis of Blockchain of Things (BCoT) Systems for Enhancing Scalability and Efficiency

Mamoon Aldmour
a030236k@student.staffs.ac.uk

A thesis submitted in partial fulfilment of the requirements of
Staffordshire University for the degree of
Doctor of Philosophy

Staffordshire University
School of Digital, Technology, Innovation and Business
United Kingdom

October, 2024

Declaration

I declare that this thesis was composed by myself, that the work contained herein is my own except where explicitly stated otherwise in the text, and that this work has not been submitted for any other degree or professional qualification except as specified.
This thesis conforms to the university research regulations and represents my work.
The research findings are documented honestly and fairly, and work attributed to other researchers has been acknowledged and referenced.

Name: Ma’moon AbdulQader Atawi Aldmour

Signature:

Date: 29/08/2024

Signed: Ma’moon AbdulQader Atawi Aldmour signature____________________
Name

Dated: 29/08/2024

Dedication

This thesis is dedicated to the loving memory of my late parents, whose dreams for my success have been a driving force throughout this journey. Though they are not here to witness this milestone, I feel their presence in every word I have written and every hurdle I have overcome. Their sacrifices and the values they instilled in me have been the foundation for this accomplishment.

To my siblings, whose unwavering belief in my abilities has been a constant source of strength. Their encouragement during moments of doubt has been a balm to my soul, reminding me of the importance of perseverance.

To my mentors and advisors, whose guidance and wisdom have been invaluable in shaping my academic journey. Your insights and encouragement have played a crucial role in my development as a researcher.

Finally, this thesis is dedicated to the memory of my dear friend, Professor Majed Abu Jaber, who left us a year ago. His friendship, support, and unwavering belief in my potential were invaluable during my journey. Professor Abu Jaber was a brilliant scholar and a compassionate soul who inspired those around him. His legacy will continue to motivate me as I strive to contribute to my field.

This work is a testament to the love, support, and inspiration I have received from all of you. Thank you for being an integral part of my journey.

Acknowledgements

Alhamdulillah, I am profoundly grateful to Allah, the Most Beneficent, for bestowing me the strength, wisdom, and perseverance to complete this academic journey. His infinite mercy and guidance have been my constant companions throughout this challenging yet rewarding process.

With heartfelt gratitude, I extend my most profound appreciation to my supervisory team. Their unwavering support and guidance, from refining my research to shaping my scholarly approach, have been the cornerstone of my academic journey.

I owe an immeasurable debt of gratitude to Dr. Rakan Aldmour, my principal supervisor. His profound insights, tireless dedication, and unique ability to challenge my thinking have shaped my research and approach to scholarly inquiry. His mentorship has been a beacon of inspiration throughout this arduous yet rewarding process.

Professor Mohamed Sedky, my second supervisor, deserves special recognition for his practical wisdom and keen eye for detail. His constructive feedback and encouragement during our countless discussions have been instrumental in refining my ideas and methodologies.

I am profoundly grateful to my external supervisor, Professor Abdallah Al-Zoubi, whose fresh perspective and expertise in the field have added invaluable depth to my work. His thought-provoking questions and suggestions have pushed the boundaries of my research, opening new avenues of exploration.

This work is a testament to the collective support of my supervisors, family, and my parents' enduring legacy. May this achievement honour their memory and serve as a stepping stone towards greater contributions to our field of study.

Published Papers

Research papers ready for submission:

1. Performance Evaluation of Blockchain of Things Cyber-Physical System Using Geth Metrics.
2. Enhancing IPFS Efficiency in Dockerized Private Networks: A Performance Evaluation Perspective.
3. Utilizing Machine Learning for Real-time Prioritization of Patient Vital Signs in Blockchain of Things Data in Intensive Care Units.

Contributions to Research Publications:

1. Al-Zoubi, A., **Aldmour, M**., Khoury, A., Al-Thaher, D. (2024).”**Blockchain of Things for Securing and Managing Water 4.0 Applications.**” International Journal of Online and Biomedical Engineering (iJOE), 20(11), pp. 4–15. https://doi.org/10.3991/ijoe.v20i11.50277

2.Al-Zoubi, Abdallah; **Dmour, Mamoun**; Sedky, Mohamed; AlDmour, Rakan. “**Blockchain Utilisation in Cyber-Physical Laboratories for Engineering Education 4.0**,” 20th International Conference on Remote Engineering and Virtual Instrumentation, 2023, Thessaloniki, Greece.

3.A. Al-Zoubi, T. Saadeddin, **M. Dmour** and L. Adi, "An Interactive IoT-Blockchain System for Big Data Management," 2022 4th IEEE Middle East and North Africa COMMunications Conference (MENACOMM), Amman, Jordan, 2022, pp. 71-76, https://doi.org/10.1109/MENACOMM57252.2022.9998263.

4. Al-Zoubi, A., **Aldmour, M.**, & Aldmour, R. (2022). “**Preserving Transparency and Integrity of Elections Utilizing Blockchain**” Technology. Journal of Telecommunications and the Digital Economy, 10 (4), 24–40. https://doi.org/10.18080/jtde.v10n4.626

Abstract

The Blockchain of Things (BCoT) ecosystem effectively tackles technological and business challenges across various domains. By utilising BCoT applications, issues related to decentralisation, data privacy, data protection, and network security are managed efficiently, enhancing operational reliability and scalability. However, recent BCoT implementations face performance issues, particularly in achieving efficient scalability, high throughput, and low latency. This research seeks to address these challenges, improve system performance, and ensure the scalability of the BCoT ecosystem.

The novel BCoT architecture showcases technological innovation by integrating a private Ethereum platform, IoT sensors, edge computing, and IPFS to create a secure, smart, and decentralised data storage system. Security within the architecture includes identity management, authentication, and access control for IoT devices, with each device assigned a unique identity. Secure communication is facilitated through MQTT and uTLS protocols, along with immutable access control rules.

The architecture's efficiency in handling large IoT data volumes was initially tested using the Random Forest classifier, which processes and prioritises sensor data in real time, achieving 99.53% accuracy in predicting conditions, assessing risk, and providing early warnings. Performance testing with the Geth Metrics tool demonstrated significant improvements over existing solutions, including a 45% reduction in latency, a 65% increase in throughput, and a 46% enhancement in Disk I/O performance. Additionally, CPU utilisation decreased by 33%, and memory usage during mining remained under 200 MB. Practical deployment and evaluation under realistic conditions showed the architecture's adaptability in executing up to 5000 transactions smoothly.

This research contributes to the field by introducing a scalable and secure BCoT architecture, adapting Blockchain mechanisms for IoT applications. The architecture's real-time, low-latency responses enhance its operational profile, offering opportunities for further research on current and future adaptations. It provides improved performance metrics, efficiency, and decision-making capabilities, impacting various practical applications. This work uniquely delivers a scalable and secure BCoT architecture, overcoming previous limitations.

List of Contents

List of Figures

List of Tables

List of Abbreviations

AI	Artificial Intelligence
AIMS	Anaesthesia Information Management Systems
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interfaces
BAN	Body Area Networks
BCoT	Blockchain of Things
BEN	Blockchain Educational Network
CDHS	Critical Data Handling Systems
CID	Content Identifier
CPL	Cyber-Physical Labs
CPS	Cyber-Physical Systems
DAG	Directed Acyclic Graph
DAO	Decentralised Autonomous Organisation
dApps	Decentralised Applications
DHT	Distributed Hash Table
DLT	Distributed Ledger Technology
DPoS	Delegated Proof of Stake
EVM	Ethereum Virtual Machine
FoF	Factories of the Future
FTP	File Transfer Protocol
HER	Electronic Health Record
HIoT	Healthcare Internet of Things
ICDHS	IoT Critical Data Handling Systems
ICU	Intensive Care Unit
IDE	Integrated Development Environment
IIoT	Industrial Internet of Things
IMS	Intelligent Manufacturing System
IoT	Internet of Things
IPFS	Interplanetary File System
KNN	K-Nearest Neighbours

KPI	Key Performance Indicator
LaaS	Laboratory as a Service
LMS	Learning Management System
MAM	Masked Authentication Messaging
MBCoT	Manufacturing Blockchain of Things
Moodle	Modular Object-Oriented Dynamic Learning Environment
MQTT	Message Queuing Telemetry Transport
P2P	Peer-to-Peer
PAN	Personal Area Networks
PLC	Power Line Communications
PMML	Predictive Model Markup Language
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof-of-Work
QoS	Quality of Service
RFID	Radio Frequency Identification
RLMS	Remote Laboratory Management System
RLP	Recursive Length Prefix
RPi	Raspberry Pi
RPi4	Raspberry Pi 4
TCP	Transmission Control Protocol
TPM	Trusted Platform Module
UDP	User Datagram Protocol
uTLS	Transport Layer Security
VLE	Virtual Learning Environment
WPAN	Wireless Personal Area Networks
WSN	Wireless Sensor Network

Chapter 1

Introduction

Integrating Blockchain technology with Internet of Things (BCoT) systems signifies a groundbreaking advancement that substantially improves performance, efficiency, and security. The decentralised architecture of Blockchain offers innovative solutions to prevalent challenges faced by IoT systems, particularly in areas such as scalability and reliability. This thesis investigates multiple facets of this integration, assessing its influence on system performance, exploring scalability solutions, and conducting a thorough performance analysis. Furthermore, it delves into the implications for individual IoT devices, illustrating how Blockchain can effectively tackle scalability issues to enhance the overall efficiency of IoT systems.

The integration of BCoT markedly boosts system performance by ensuring data integrity and reinforcing security measures. The decentralised ledger inherent in Blockchain mitigates the risks associated with a single point of failure, which is a significant vulnerability in conventional centralised IoT architectures. This integration also promotes real-time processing and validation of transactions, thereby diminishing latency concerns and assuring the accuracy and timeliness of data. A critical challenge within distributed computing is the scalability of IoT systems, which traditionally rely on centralised architectures that need help managing the vast amounts of data generated by interconnected devices. However, Blockchain's decentralised framework presents viable solutions to these scalability challenges by facilitating horizontal scaling—adding additional nodes to the network to accommodate increased data loads—thus enhancing system efficiency and responsiveness irrespective of the number of connected devices. By incorporating Blockchain into IoT architectures, systems can expand by evolving operational requirements, fostering a more extensive and resilient network.

An in-depth analysis of BCoT systems and their architectures reveals numerous performance advantages, including improved data security that ensures recorded information remains unchanged and maintains a reliable and verifiable history of events. This characteristic cultivates trust and dependability within the system. Moreover, this integration reduces operational costs and enhances data verification processes. Smart contracts can automate various operations, further optimising system efficiency. While the overarching system benefits from Blockchain integration, individual IoT devices undergo significant transformations. These devices gain greater independence, lessening their dependence on central servers for data validation and transaction processing. This shift enhances device autonomy while alleviating network congestion and potential bottlenecks. Blockchain technology elevates IoT system efficiency by establishing a secure and dependable data exchange and transaction processing framework. Smart contracts facilitate automatic and transparent operation execution, minimising the necessity for manual intervention and reducing errors. Consequently, this results in quicker processing times and heightened trust among stakeholders.

Blockchain integration adeptly addresses scalability challenges within IoT systems. The system can manage increased data loads by distributing the ledger across multiple nodes without sacrificing performance. This decentralised methodology prevents bottlenecks while ensuring sustainable growth. Additionally, consensus mechanisms like Proof of Authority (PoA) can enhance scalability by lowering the computational resources required for transaction validation. This thesis elucidates how integrating Blockchain technology with IoT systems enhances overall performance and provides innovative solutions to longstanding challenges related to scalability and efficiency. The findings underscore the transformative potential of BCoT systems in various applications, paving the way for future advancements in this domain.

1.1 Blockchain Technology

Blockchain technology has emerged as a ground-breaking innovation in digital record-keeping and data management, fundamentally operating as a distributed, decentralised ledger that securely records transactions across a network of computers without the need for a central authority. Initially introduced as the underlying technology for Bitcoin, Blockchain has transcended its origins in cryptocurrencies to find applications across various sectors such as supply chain management, healthcare, voting systems, and identity verification. The core concept of Blockchain involves a peer-to-peer network where each participant maintains a copy of the entire ledger, with transactions grouped into cryptographically linked blocks to form an immutable information chain. This structure ensures data integrity, transparency, and immutability, making Blockchain particularly valuable for applications requiring high levels of security and trust (Attaran, 2020). One of the key features that sets Blockchain apart is its ability to eliminate the need for intermediaries in many processes, potentially reducing costs and increasing efficiency across different. Smart contracts, which are self-executing agreements with terms directly encoded into code, further enhance the capabilities of Blockchain technology by automating complex transactions and agreements. These smart contracts are primarily used for general-purpose computations within a Blockchain or distributed ledger. As Blockchain technology continues to evolve, it promises to reshape how transactions are conducted, data is managed, and trust is established in the digital age, potentially leading to more transparent, efficient, and secure systems across various domains of society and business (Huang, et al., 2018).

The development of Blockchain technology is closely intertwined with the evolution of smart contracts, which have become a focal point of interest in academia and industry (Tian & Chen, 2022). Smart contracts leverage the inherent characteristics of Blockchain, such as immutability, transparency, and decentralisation, to offer a secure and reliable solution for data management (Kishor, 2023). These contracts are designed to automate and enforce contract execution, providing a platform for applications that run on a peer-to-peer network rather than a single server (Ozpinar & Kalinyazgan, 2024). Integrating Blockchain technology and smart contracts enhances data security and enables process automation throughout supply chains (Nishani & Barkhi., 2021).

Blockchain's decentralised nature and secure data storage capabilities have led to its exploration in various sectors, including electric vehicles and charging pile management. The security model proposed for this application is based on the Blockchain ecosystem, highlighting the potential for Blockchain to enhance security in critical infrastructure systems (Zheng, et al., 2020). Furthermore, the use of Blockchain in spectrum-sharing transactions for multi-operator wireless communication networks demonstrates the technology's versatility in facilitating complex transactions across different industries (Raza, et al., 2023). The application of Blockchain in supply chain management, particularly in agricultural food supply chains, showcases its potential to address the challenges of globalisation and intricate regulatory policies (Zhuang., et al., 2023). Despite Blockchain technology's numerous advantages, challenges such as scalability, energy consumption, and regulatory frameworks remain significant hurdles to its widespread adoption (Nissl, et al., 2020). Scalability, in particular, has become a pressing issue as Blockchain technology is increasingly integrated into various applications (Lee & Choi, 2020). Efforts to address these challenges, such as optimising Blockchain for smart contracts and exploring cross-Blockchain smart contracts, reflect the ongoing research and development in the field. Additionally, identifying security vulnerabilities in smart contracts underscores the importance of ensuring the integrity and reliability of Blockchain-based systems.

1.2 IoT

The IoT has become integral to various sectors, including healthcare, smart cities, engineering, and more (Mohammed & Hasan, 2023). This interconnected network of physical devices, vehicles, appliances, and other items embedded with sensors, software, and connectivity enables the seamless exchange of data and information (Kim, 2024). In healthcare, IoT technology has revolutionised patient care by facilitating the connectivity of devices to the Internet, creating what is known as the Internet of Medical Things (IoMT) or the Healthcare Internet of Things (HIoT) (Jaleel, et al., 2023). By leveraging IoT, healthcare systems can track, monitor, and communicate health data in real time, leading to improved outcomes and personalised care (Anyanwu, 2024). Integrating IoT technologies in healthcare has shown immense promise, particularly in paediatric populations, by enhancing patient care and treatment outcomes (Olorunsogo, 2024). IoT-based health monitoring systems have emerged as transformative tools, especially in tracking the health of elderly individuals, offering a paradigm shift in healthcare delivery (Kumar, 2024). Additionally, the network of medical devices and sensors in the healthcare field, known as the Internet of Healthcare Things (IoHT) or Internet of Medical Things (IoMT), has facilitated rapid data transmission and improved healthcare resource utilisation (Al-hajjar & Al-Qurabat, 2023). Security and privacy are critical considerations in IoT applications, especially in healthcare settings. Researchers have explored steganography, chaotic functions, and encryption methods to ensure privacy-preserving innovative healthcare systems (Rostam., et al., 2023). Lightweight cryptographic systems have been studied for their impact on IoT-based applications, emphasising the need for secure communication and data exchange in IoT environments (Kim, 2024). Furthermore, Blockchain technology has shown promise in enhancing data security and efficient information sharing in wireless networks, addressing the growing cybersecurity concerns in IoT applications (Zhou, et al., 2024). Machine learning and AI have been increasingly integrated into IoT systems to enable predictive and preventive healthcare solutions. When combined with IoT, these technologies offer personalised health management, chronic disease diagnosis, and efficient healthcare services (Jaleel, et al., 2023). Deep learning and AI-powered smart health monitoring systems have demonstrated significant potential in analysing health data and providing valuable insights for healthcare professionals (Philip, et al., 2023). Moreover, nature-inspired algorithms have been explored to optimise security and enhance healthcare services in IoT-based applications, showcasing the diverse applications of IoT in healthcare (Amiri, et al., 2024). The Internet of Things has transformed healthcare by enabling real-time monitoring, personalised care, and efficient data exchange. BCoT and advancements in AI, machine learning, and security measures have paved the way for innovative healthcare solutions. As IoT continues to evolve, its impact on healthcare will drive further advancements in patient care, disease management, and overall healthcare delivery.

1.3 Applications of BCoT

BCoT offers a promising avenue for enhancing performance and scalability in various applications. Numerous studies have explored this intersection, emphasising merging these technologies' potential benefits and challenges. One crucial aspect highlighted in the literature is Blockchain's capacity to improve security in IoT networks. IoT devices can securely exchange data using Blockchain's decentralised and immutable ledger system, ensuring transparency and reducing fraud risks (Chand, et al., 2024). This security feature is vital in IoT environments where data integrity and confidentiality are paramount (Burgos & Pustišek, 2024). Furthermore, the integration of Blockchain with IoT has the potential to enhance scalability. Blockchain technology provides a distributed approach to data management, which can assist in efficiently handling the vast amounts of data generated by IoT devices (Tiruvayipati., et al., 2024). This scalability is crucial for IoT applications that necessitate real-time processing of data streams from numerous interconnected devices (Sharma., et al., 2024). Blockchain's ability to streamline data exchanges in IoT networks can enhance scalability by offering a secure and transparent framework for managing data flows (Venkatesh, et al., 2024). Moreover, the synergy between Blockchain and IoT can lead to advancements in performance. By integrating Blockchain technology with IoT devices, processes such as firmware updates and data transactions can be optimised for efficiency. The utilisation of Blockchain verification mechanisms, such as Merkle trees, can enhance the fidelity and speed of data transfers in IoT networks, thereby improving overall performance (Shin & Jeon, 2024). Additionally, incorporating Blockchain in IoT architectures can ensure the safety and scalability required for seamless integration (Thakur & Sehgal., 2024). Integrating Blockchain with IoT networks has demonstrated promise in enhancing intrusion detection system (IDS) performance in cybersecurity. IoT environments can benefit from improved threat detection and response mechanisms by integrating Blockchain technology into IDS frameworks, strengthening cybersecurity defences. This integration can enhance the overall performance of IoT systems by ensuring the integrity and security of data exchanges (Ahakonye, et al., 2024). Furthermore, Blockchain applications in IoT can revolutionise supply chain traceability by establishing a secure and transparent system for tracking goods and materials. This integration can improve supply chain management efficiency by leveraging Blockchain's decentralised nature to guarantee the authenticity and reliability of product information. By providing a tamper-proof record of transactions, Blockchain technology can optimise supply chain processes and enhance overall performance (Kee, et al., 2024). Integrating Blockchain and IoT can also address challenges such as Distributed Denial of Service (DDoS) attacks by implementing multi-layer security frameworks. Blockchain solutions designed to enhance security and privacy in IoT environments can mitigate the risks posed by cyber threats, improving IoT networks' overall performance and reliability. By leveraging Blockchain technology, IoT devices can be safeguarded against malicious activities, ensuring uninterrupted operations and enhanced performance (Sharma & Rohilla, 2024).

Integrating Blockchain and the Internet of Things (BCoT) holds significant potential for enhancing performance and scalability in various domains. IoT applications can benefit from improved data management, enhanced cybersecurity, and streamlined processes by leveraging Blockchain technology's security, scalability, and performance-enhancing features. The synthesis of these technologies presents a transformative approach to optimising IoT networks and unlocking new possibilities for innovation and efficiency.

1.4 Proposed BCoT Architecture Design and Implementation

This thesis introduces a novel BCoT architecture design that seamlessly integrates IoT devices with Ethereum Blockchain technology. The architecture comprises a private Ethereum platform, IoT sensors, and edge computing capabilities, AI, and IPFS storage, forming a secure and decentralised data management solution. Raspberry Pi devices function as Blockchain nodes, while various microcontrollers serve as sensor interfaces, facilitating comprehensive IoT integration. Before Blockchain integration, the system employs an edge-computing algorithm for efficient local data processing and IPFS storage. The design incorporates robust identity management and secure communication protocols to enhance security. The efficiency of the BCoT architecture in processing large volumes of IoT data was initially evaluated using a machine learning classifier known as the Random Forest classifier. This classifier can process and prioritise data records from sensors in real-time, achieving an accuracy of 99.53% in predicting various conditions, assessing risk levels, and providing early warnings. The performance assessment, conducted using machine learning classifiers and Blockchain metrics tools, indicates significant enhancements in system efficiency, such as reduced latency, increased throughput, and optimised resource utilisation. Furthermore, the study evaluates the performance of IPFS within containerised environments, demonstrating superior latency and resource management compared to traditional file transfer methods.

This research contributes valuable insights into the potential of Blockchain-IoT integration in advancing CPS, highlighting enhanced performance and security capabilities.

1.5 Research Aim and Objectives

The main research aim and objective is to propose a novel architecture for the life cycle of data gathered from sensors, particularly Remote Lab or Vital Signs in an ICU room, to the Blockchain for storage and processing purposes. The specific objectives are to:

- Conduct a comprehensive literature review on the BCoT to critically evaluate the current state of integration between Blockchain and IoT technologies.
- Analyse the application of Blockchain technologies within BCoT frameworks, examining their inherent limitations and challenges to identify areas for potential improvement and innovation.
- Develop a novel case-based BCoT architecture. This architecture will facilitate the systematic data collection from IoT devices through web services and data files, ensuring interoperability and efficient data management.
- Conceptualize and implement a novel Blockchain-based storage architecture for BCoT-generated data. This architecture will leverage the IPFS for distributed storage while maintaining data chronology and integrity through Ethereum smart contracts, ensuring the security and reliability of the stored data.
- Rigorously assess the scalability and performance characteristics of the proposed Blockchain-based architecture through comprehensive testing and analysis. This evaluation will focus on the system's capacity to handle increasing workloads and maintain optimal performance under diverse operational conditions, ensuring alignment with predefined functional and performance requirements.

1.6 Research Questions and Hypotheses

- **Question 1:** How can Blockchain technology and associated decentralised systems be effectively integrated to create a robust and scalable infrastructure for storing and retrieving diverse data types in a distributed environment?

  Hypothesis: Blockchain technology, when integrated with decentralised systems like the InterPlanetary File System (IPFS), will significantly enhance the robustness and scalability of data storage and retrieval in distributed environments by ensuring data integrity, transparency, and accessibility without a single point of failure. This will enable efficient management of diverse data types across a distributed infrastructure.
- **Question 2:** What is the optimal architectural design for a BCoT ecosystem that efficiently manages IoT-generated data, and how does the synergy between on-

chain Ethereum Blockchain and off-chain storage solutions like IPFS contribute to system performance and scalability?

Hypothesis: The optimal BCoT (Blockchain of Things) architecture for managing IoT-generated data involves a hybrid approach using Ethereum Blockchain for on-chain transactions and IPFS for off-chain data storage. This leads to improved system performance in terms of transaction throughput and reduced latency. The synergy between these two systems will significantly enhance scalability and provide secure, tamper-resistant data management for IoT ecosystems.

- **Question 3:** How does implementing edge computing algorithms in conjunction with Blockchain technology impact the scalability, latency, and overall performance of the BCoT system, and what are the potential implications for real-time data processing in IoT-intensive environments?

  Hypothesis: Integrating edge computing algorithms with Blockchain technology in the BCoT system will improve scalability and reduce latency, enabling faster real-time data processing in IoT-intensive environments. This hybrid architecture will distribute computational loads across the network, alleviating centralised bottlenecks and enabling the efficient handling of large-scale IoT data flows.

- **Question 4:** How can AI-driven algorithms optimise the prioritisation of critical data in BCoT architecture, and what is the impact of real-time evaluation and decision-making on system efficiency, security, and scalability for healthcare applications?

  Hypothesis: AI-driven algorithms, when incorporated into BCoT architecture, will enhance the prioritisation of critical data, especially in healthcare applications, by enabling real-time evaluation and decision-making. This will improve system efficiency, enhance security measures through more accurate anomaly detection, and ensure scalable data management for time-sensitive healthcare scenarios.

1.7 Research Gap

Integrating Blockchain technology, IoT devices, and AI systems has the potential to revolutionise healthcare and engineering education. However, there is a significant research gap in addressing the limitations of scalability, efficiency, security, latency, and throughput that hinder the widespread adoption and impact of these technologies in critical sectors.

The current healthcare and CPL infrastructures need help managing the increasing volume of data generated by IoT devices. This is leading to scalability issues and congestion within Blockchain networks. It is challenging to ensure data integrity, privacy, and secure communication among IoT devices, Blockchain networks, and AI systems, which often compromises security and efficiency. In addition, Blockchain-based systems' high latency and limited throughput pose significant obstacles to real-time data processing and smooth integration. These factors, such as healthcare data monitoring, prioritising and educational simulations, are crucial in time-sensitive situations. This research aims to fill this research gap by developing a scalable, cost-effective, and secure architecture to combine the potential of Blockchain, the IoT, and AI technologies for digital health and CPL. Overall, the research will leverage the advantages of IPFS for data that needs to be stored decentralised, the MQTT protocol for optimal data communication in real-time, AI technologies for data processing and predictions, and lastly, the Blockchain for securing the management of data while also ensuring the transparency of all parties involved on the Blockchain network. These technologies can be integrated to address scalability problems, improve efficiency and security, reduce latency and throughput problems in real-time data processing simultaneously, and contribute to health care and education (Arachchige, et al., 2023) (Moudoud, et al., 2021) (Confais, et al., 2017).

1.8 Integrating BCoT in Education and Healthcare: A Novel Architecture for Secure and Efficient Systems

The proposed innovative architecture in this thesis integrates BCoT technology with two distinct applications: (i) a Learning Management System for Laboratories 4.0, and (ii) a Machine Learning-Driven Real-Time Prioritization of ICU patient vital signs. The BCoT architecture offers a secure, decentralised management system for remote laboratories by utilising Blockchain technology to address issues such as data integrity, access control, and resource allocation. This is achieved through smart contracts that automate lab processes, ensure record audibility, and facilitate smooth interactions between students, teachers, and lab equipment, enhancing remote lab experience. The Laboratories 4.0 application innovatively uses Blockchain to create a trustless and transparent environment for remote lab management, allowing secure, auditable, and decentralised execution and management of remote experiments. This approach addresses challenges in remote education, such as proving student presence, fair resource allocation, and experiment data integrity.

For the Machine Learning-Driven Real-Time Prioritization system, the BCoT architecture is adapted to manage and secure critical patient data in the ICU. This system combines machine learning algorithms with Blockchain technology to improve the analysis of vital signs data, prioritising it in real-time to support healthcare providers in critical care scenarios. Machine learning aids in detecting critical patterns and anomalies in patient vitals, while Blockchain ensures data integrity and secure sharing among healthcare providers.

The architecture novelty lies in its real-time machine-learning analytics combined with Blockchain-based data management, enabling intelligent prioritisation of patient data while safeguarding against data corruption and security breaches. The architecture's ability to update patient data in real time and the immutability of Blockchain records mark a significant advancement in ICU patient monitoring and care. The primary distinction in BCoT application between the two cases is their design for different purposes and contexts. The Laboratories 4.0 system enhances educational experiences and manages remote resources with transparency and fair access. In contrast, the ICU priority system emphasises critical healthcare data management, prioritising speed of analysis and response through machine learning to aid decision-making in healthcare environments.

The applications discussed illustrate how BCoT architecture can be tailored to address diverse challenges across different domains. By applying the core BCoT technology (Blockchain and IoT integration) to specific use cases, this research demonstrates how BCoT can transform the education and healthcare sectors, making them more secure, efficient, and intelligent.

1.9 Contribution

- A study examines two real-world demonstrations of IoT and Blockchain technology, a remote lab management system and machine learning-based real-time prioritisation of

ICU patient vital signs using the Ethereum platform. This required physically embedding IoT devices in the Ethereum platform and measuring system latency, throughput and energy consumption of IoT devices as part of the application's performance analysis.

- In this thesis, a novel BCoT architecture was proposed that seamlessly integrates IoT devices with devices based on Ethereum Blockchain technology. This architecture incorporates IoT sensors, edge computing capabilities, AI capabilities, IPFS storage, and a private Ethereum platform. This architecture prioritises critical data in IoT systems and stores it using Blockchain. A decentralised MQTT broker concept is integrated into the BCoT architecture, providing a security layer for integrating IoT and Blockchain, contributing to the resilience and scalability of the BCoT. This Thesis presents the BCoT architecture, which is based on comprehensive research to efficiently handle excessive amounts of IoT data. A Random Forest classifier is used to process and analyse the IoT data and achieve an accuracy of 99.53% in forecasting the conditions, rating the risk and generating an early warning.
- The performance of the BCoT architecture is evaluated against benchmarks in different domains. Significant improvements in the latency, throughput and resource utilisation of the BCoT over existing benchmarks are measured. This Thesis presents the Integration of IPFS and Edge-computing into the BCoT architecture, which can potentially enhance the overall performance of the BCoT. The Interaction of IPFS with the BCoT shows a superior performance of IPFS compared to existing file transfer methods in a containerised environment. The research contents in this thesis contribute to the understanding of Blockchain integration in CPS. This work can potentially build upon foundations for further research into IoT-Blockchain Integration. It can potentially enhance the performance and security of existing CPS.

  The performance analysis is provided, including measurements of Disk space usage, Memory usage, CPU Utilization, energy consumption, and transaction-related statistics using modern technologies like InfluxDB and Grafana for different IoT-Blockchain network implementations over Wi-Fi.
- Built a highly resilient, scalable, and efficient content storage and delivery system by integrating IPFS, IPFS Cluster, and Docker and using hyper-parameter optimisation.

The system addresses challenges such as data redundancy, availability, and ease of management. It also highlights the system's effectiveness through experiments that measured the latency of file reading and writing operations. The experiments demonstrated a significant reduction in latency, indicating the system's ability to handle content delivery effectively.

1.10 Thesis Organisation

The PhD research started by combining IoT and Blockchain technologies. The result is this thesis, divided into eight chapters. Each chapter deals with one aspect of this innovative combination.

The first chapter starts with an introduction to the problem that was the focus of the research and explains what the author aimed to achieve, what objectives were pursued, and what research questions were asked or pursued along the way. The first chapter also starts to make a case for the work and why it matters in terms of where it fits into and contributes to the literature. The literature review builds upon the introduction to present the core concepts. First, the operation of Blockchain technology is presented, distinguishing between permissioned and permissionless networks and among various consensus mechanisms. Next, prominent Blockchain platforms like Ethereum, IOTA, Hyperledger Fabric, etc., and off-chain storage options like IPFS are analysed. This is culminated by a critical analysis highlighting the existing research gaps, laying the study's foundation.

The research methodology chapter includes the epistemological and methodological foundations of the research and the rationale for the study, meaning the description of the experimental methods used, the time horizon, the techniques and procedures for data analysis, and a complete guide of the strategies for the development of rigour and validity of the research. The fourth chapter explains the design and optimisation of the novel BCoT architecture. Within this section, the design phase, the initialisation phase, the test phase and the deployment phase are discussed. The design phase covers the design of BCoT from scratch, explaining the integration of Ethereum Blockchain and Proof of Authority (PoA) with Raspberry Pi nodes, edge processing, data collection and storage. The initialisation phase describes the overall system and the protocols running on the BCoT components. Finally, the efficiency and security of Ethereum's Clique PoA protocol for BCoT are analysed in the test phase. Chapter 5 shows how the remote laboratory management system has evolved from Lab 1.0 to Lab 4.0. It proposes a Blockchain-based system to handle remote labs, comparing it with the traditional systems. The results and implications of the novel approach are presented and elaborated on. Moreover, the future of Blockchain in lab management is discussed. The sixth chapter proposes an algorithm for real-time prioritising ICU patients' vital signs using machine learning as part of the Blockchain networks. It presents the data prioritising algorithm and its steps, normalisation, and implementation. The algorithm demonstrates how machine learning can add value and effectiveness to the proposed solution.

Chapter 7 is dedicated to performance analysis of the integration of IoT with Blockchain technology. It also tracks the bottlenecks of various transactions. The protocols and tools used to monitor performance are described. The integrated system is evaluated for performance. In the end, a discussion is presented on integrating IPFS and private Ethereum Blockchains to enhance the system's scalability, privacy, and trust.

The ending is an abstract in chapter eight summarising the main findings and delving into the implications for practice and theory. The study's limitations and recommendations for future research are discussed. Thus, this thesis sheds light on several significant insights and solutions that could be applied to different domains, especially in healthcare and laboratory management. This endeavour is challenging but rewarding.

Following Chapter 2, the Literature Review and the primary functioning mechanism of Blockchain are described, as well as the difference between permissioned and permissionless networks and their consensus mechanisms. Prominent Blockchain platforms like Ethereum, IOTA and Hyperledger Fabric are addressed, as are their off-chain storage solutions like IPFS, with a critical analysis at the end. The analysis identifies the gaps in the current research literature and sets the context for the study.

Chapter 2

Literature Review

2.1 Introduction

The exploration of distributed ledger technology, particularly Blockchain, reveals its transformative potential across various sectors. This chapter delves into the foundational aspects of Blockchain, beginning with a comprehensive overview of distributed ledger technology and its evolution. A distinction is made between permissioned and permissionless networks, highlighting their unique characteristics and applications. The analysis extends to consensus mechanisms, which are pivotal in ensuring the integrity and security of Blockchain transactions. Further investigation into Blockchain platforms elucidates their operational frameworks and the role of off-chain solutions like the IPFS. The integration of Blockchain with emerging technologies such as artificial intelligence and the IoT is examined, showcasing the synergistic benefits that enhance scalability and efficiency. The discussion also encompasses the implications of Blockchain in educational contexts, particularly in engineering education, where it supports innovative learning paradigms. The convergence of IoT, big data, and Blockchain is critically analysed, emphasising how this triad can address scalability, throughput, and latency challenges in BCoT systems. The evolution from traditional laboratory systems to modern remote lab frameworks illustrates the impact of these technologies on educational practices. By synthesising these elements, a clear narrative emerges about the ongoing advancements in Blockchain technology and its applications in various domains, setting the stage for further research and development in this dynamic field.

2.2 Introduction to Distributed Ledger and Blockchain Technology

2.2.1 Distributed Ledger Technology (DLT)

DLT is the next iteration in database architecture, allowing for secure, transparent, real-time record-keeping across distributed networks without a trusted central authority (Chowdhury, et al., 2019). DLT involves a peer-to-peer network replicating and disseminating data across each node and acts as a trusted responder. If one part of a network fails, the other nodes can continue to perform and deliver data securely. A distributed ledger operates in a way that eliminates the need for a central location. Instead, the ledger's data is replicated across interconnected nodes, creating a trustless system. This removes the reliance on a centralised model found in traditional databases, where trust in the central authority is required.

DLT is entirely tamper-proof, making it immutable once data enters the system. No one can alter or delete it, as the network automatically prevents any attempts to modify or erase data. A DLT is a way of storing much more robust data than previous systems. It is a self-updating system that no one can suborn. It is a system in which the source of truth can never be erased or altered, and no records of discredited people are ever removed. A DLT can run successfully even if bad actors compromise some – or nearly all – of the nodes in the network because it has a consensus mechanism that ensures that the network always agrees with itself. The best-known consensus mechanism is Proof of Work, which works on the algorithms that Bitcoin miners solve to update their ledger. In fact, most Blockchain systems use this consensus mechanism (Zhou, et al., 2022). However, this consensus mechanism can be expensive in terms of energy to update the network ledger. A viable alternative mechanism is known as PoS. In PoS, economic incentives are given to nodes who stake or 'bond' their cryptocurrency to validate network transactions, thereby securing them. DPoS and PoA are also consensus mechanisms, and their many nuances and varieties of combinations have been explored recently. These consensus mechanisms gather validations through methods such as voting systems that create hash functions (i.e., connect old and new blocks of data, each hash function adding its block to the global new hashing of the chain), Merkle trees (unique data structures used to verify information), and cryptographic digital signatures.

On a DLT system, every protocol node validates the same actions on its own data copy. These work through asymmetric cryptography, protecting validators and ensuring data authenticity. These systems use algorithms such as 'cryptographic hash functions' that take in data as input and anonymise it into a simple signature so that a hashing function can be created to re-access it, similar to our fingerprints. Cryptography is also used through various encryptions, with 'private keys' of data known only by a sender to validate transactions, plus ‘public keys’ shared with a receiver to protect them. Across decentralised systems like Bitcoin, cryptographic algorithms, such as hashes and signatures that utilise cryptography, run on every one of the system’s nodes, distributed across a peer-to-peer network of computers around the internet. It would be nearly impossible to shut down the entire system because there is no central point to attack or shut down. Instead, key functionality is replicated and run by thousands of nodes spread across the globe (Hussein, et al., 2023).

2.2.2 Blockchain Technology

Blockchain architecture is ingenious because, by design, it attempts to create a decentralised system that contrasts significantly with centralised models. This architecture enables the creation of an unalterable digital ledger, which distributes transparent, secure transactions among peers. The core idea behind Blockchain architecture dates back to 1991.

Its invention aimed to ensure the simple yet fundamental requirement of a system allowing timestamping for any digital documents: in other words, a system that could not be backdated and that could not be tampered with. This conception of a system led to the core structure of Blockchain architecture as we know it today. Still, it remained theoretical in this form for many years until 2008, when Satoshi Nakamoto changed the game by creating Bitcoin, the first Blockchain-based cryptocurrency (Nakamoto., 2009). This leap in a single bound transformed the Blockchain architecture from an abstract concept into a working tool.

Blockchain technology has recently attracted enormous attention and acclaim for its potential to revolutionise large companies and sectors such as healthcare. Its main particularity lies in its decentralised information management architecture, which guarantees transparency and immutability of transactions and facilitates data flow. Blockchain potentially holds excellent promises for healthcare with its capacity to address some significant problems of the Organisation for Economic Co-operation and Development: interoperability, data fragmentation, medicine supply chain management, patient and physician agency, data quality and quantity, medical research and data security and integrity (Attaran, 2020). This technology provides a decentralised, transparent architecture for guaranteed secure data storage, sharing and access control (Ali, et al., 2023)

(Adeghe, et al., 2024). In this regard, Blockchain can enhance data security and integrity, transparency, and efficiency of operations, providing significant gains for healthcare (Atadoga, et al., 2024) (Kumarswamy & Athikatte., 2024). Blockchain technology and its decentralised architecture provide intact data from source to destination; patients can quickly transfer their medical records to the hospital or clinics they want to visit (Calik & Bendechache, 2024). Blockchain technology, safeguarding the patients' data stored in a distributed repository, enhances medical resource traceability in the healthcare supply chain (Quayson, et al., 2024).

Adding to the former application, Blockchain technology restructures healthcare by integrating IoT in medical applications, securing traditional practices, data management, data sharing, patient remote monitoring and drug analysis (Kamangar, et al., 2023). Furthermore, the security and privacy of patient data in healthcare are critically enhanced by Blockchain technology. This is achieved through the immutable storage capabilities of distributed ledger technology, which ensures that patient information remains tamper-proof and prevents any unauthorised alterations by physicians, thereby eliminating the possibility of data repudiation (Handayani, et al., 2023) (Arul & Renuka., 2023).

In addition, the decentralised management of transaction data through Blockchain technology offers a secure system for storing and retrieving healthcare data in cloud computing environments (Anil & Kamble, 2023). Blockchain application to healthcare information exchange permits decentralised data protection, safeguarding against particular risks and optimising decision-making processes, patient outcomes, and automation of healthcare professionals through the integration between Blockchain and machine learning (Kumar., et al., 2023).

Moreover, healthcare systems using Blockchain technology enhance the security and privacy of patient data, streamlining the healthcare data-management system by harnessing smart contract systems able to control information flows and prevent data sharing (Shava. & Mhlanga., 2023). Blockchain delivers structure and security to organisational data, ensuring the safety and reliability of healthcare systems, a salient feature of healthcare (Alhamzah, et al., 2022).

On the other hand, Blockchain seems to be a promising technology for integrating with CPS to achieve better security and operation. A research study identified Blockchain technology as incredibly useful in improving CPS performance and security. The reason for this is explained by the integration of Blockchain and machine learning for robust authentication, which helps address the issues of data management and storage and makes CPS highly susceptible to external attacks (Khalil, et al., 2021).

In CPS, which can encompass large-scale, dynamic interactions and control loops, decentralisation is advantageous, and indeed, Blockchain is ideally suited to the application. Aside from a general overview of CPS applications of Blockchain, some recent papers offer more specific overviews (Khalil, et al., 2021). For example, an extensive review paper addresses the security and operation of CPS enabled by Blockchain. It describes the applicable applications of Blockchain across all categories of operations, describing it not only in terms of its usability for security but also concerning the inherently additional protections afforded by it while highlighting the constraints imposed by Blockchain and simultaneously retaining the central aspects of CPS (Rathore, et al., 2020). The combination of Blockchain and machine learning approaches is also discussed to enhance CPS security and provide a two-layer defence against external attacks. For example, a novel approach utilises deep learning, Blockchain and 6G IoT models with sensor-based health monitoring for patients. The sensor collects, examines, and transmits data (Rahman, et al., 2024).

Blockchain, despite the tremendous hype, has several shortcomings. First, the biggest is that of scalability (Kumarswamy & Athikatte., 2024). This refers to the number of transactions that can happen on the Blockchain as the volume of records on it grows. Blockchain also has significant issues in terms of energy consumption. The process of mining for a cryptocurrency requires considerable energy. Besides, in particular, Blockchain innovations face a myriad of regulatory problems because of the heterogeneity of legal frameworks among different geographic jurisdictions.

This heterogeneity, in addition to being a substantial obstacle for Blockchain systems' uniform application and governance, also gives rise to interoperability problems because different Blockchain technologies do not always work with each other and across different Blockchain platforms. All these factors together mean that Blockchain technologies are not easily integrated into existing legal and technological frameworks (Ahmed G. Gad, 2022).

Solutions for these considerations are also making their way to the Blockchain, notably through more practical approaches to address the scalability problem, such as the adoption of sharding (i.e., splitting the database into smaller parts) or off-chain procedures (i.e., intermediary code that eliminates a large part of the data at risk from being recorded in Blockchain), and more energy-efficient consensus mechanisms such as PoA, as a solution to the energy consumption issue, and a single, global regulatory framework for a regulatory challenge. Cross-chain protocols and standards can pave the way to interoperability (Atadoga, et al., 2024).

AI, IPFS, and PoA consensus mechanisms are three exciting solutions to improving the scalability of Blockchain technology. Blockchain scalability can be enhanced by applying AI technology to optimise many processes, including choosing configuration settings for the architecture or optimising the consensus mechanism. Machine learning algorithms can optimise the configurations of Blockchain settings, such as the block size and interval, or choosing the block producer, to deal with the dynamics and prominent dimensionality characteristic of systems like the IIoT and to optimise the trade-offs according to the scalability trilemma (Rožman, et al., 2022).

Moreover, AI can optimise consensus mechanisms, data management, improved storage and access, data analytics, and transaction processing. IPFS, a distributed file storage and sharing system, is the second technology that enhances Blockchain technology's scalability. Offload the data storage from the Blockchain to IPFS to minimise the storage limit and burden on the Blockchain. It allows for the secure storage of large datasets, and improved data retrieval and sharing applications benefit IoT and smart contracts (Ahakonye, et al., 2024). For example, a cold supply chain system deployed in connected trucks uses smart and multiple IoT sensors to monitor everything while delivering fresh goods.

The third technology is PoA, a consensus mechanism that provides a scalable and cost-effective solution to the existing native consensus mechanisms in Blockchain technology, such as PoW and PoS. PoA enables transactions to be approved only by a limited number of known and trusted validators. This mechanism is widely utilised in private and consortium Blockchain (Sharma & Rohilla, 2024). PoA can improve transaction throughput and lower latency, enabling Blockchain technology in applications requiring better performance, efficiency, and scalability.

The Blockchain system has internal diagnostics that protect it from incorrect transactions and place data in only one place where everyone can view it (Khandelwal, et al., 2021). Blockchain technology is the combination of three technologies; these include:

1. Private Key cryptography kicks off transactions on the Blockchain.
2. P2P communication – the decentralised communication between two peers (called nodes) via a network of many nodes where multiple copies of information are stored on the nodes (as verified transactions).
3. Smart contracts that define the protocols of the transaction executed by transaction initiators. The Blockchain is a sequence of blocks connected via the hash pointer. Each block is recorded with the previous block's hash, which makes the data immutable and aids the nodes (connected to the Blockchain network) in tracking its flow.

The immutability of Blockchain technology is a fundamental property that stems from its decentralised and distributed nature. Each block in the Blockchain is cryptographically linked to the preceding block through a unique hash value derived from the data contained within that block. Consequently, any alteration or modification to the data in a particular block would change its corresponding hash value. This change would propagate through the entire network, causing a mismatch with the subsequent blocks in the chain, as all nodes (participants) in the Blockchain network maintain a copy of the ledger.

For an adversary to successfully tamper with the data stored on the Blockchain, they would need to recalculate the hash values of the targeted block and all subsequent blocks in the chain. This task is computationally infeasible and practically impossible due to the immense computational power required to overpower the collective computational resources of the entire network. As the network grows more significant, the difficulty of such an endeavour increases exponentially, rendering the Blockchain inherently resistant to unauthorised modifications. This intrinsic characteristic of the Blockchain architecture ensures the integrity and immutability of the stored data, making it an attractive solution for applications requiring high data security, transparency, and trust. Initially, Blockchain technology was applied to the real-time monitoring of transactions used by Bitcoin cryptocurrency. Blockchain has been widely employed in many applications, and its distinctive features are decentralised, security-based, reliability-based, privacy-based, and data-based. In particular, Blockchain has been applied to various applications, including Healthcare, Logistics, Supply Chain, IoT, and e-government (Moosavi, et al., 2021).

Blockchain can be classified into the following types: Private, Public, and Consortium. A public Blockchain is an open, unrestricted platform where anyone can join a network without permission. The transactions in the Blockchain are public, and users can check and validate them. A private Blockchain cannot guarantee that participants on a list of allowed organisations will be connected to the Blockchain network. The number of participants allowed to be involved in the confirmation of transactions is limited.

Consortia Blockchain is a semi-decentralized system in which organisations participate in network operations. Participating organisations can become nodes on the network and verify and share the transaction information (Tanwar, et al., 2020). The working principle of the Blockchain is described in the diagram given in Figure (1).

The user first creates a smart contract transaction in a Blockchain network. The user sends the transactions to all the nodes (P2P computers) in a P2P network. All the transactions are pending and paid by pool. All the blocks are encrypted with hashes, and the transactions are checked and stored in these blocks. There is a mining process that requires competing by nodes in the network. Miners select the transactions from a pool and must verify them instead of using a fixed validation rule given by the Blockchain network's creators. Once the node successfully mines the block, a new block will be generated and broadcast to the network nodes; after this block is finally mined, this block is added to the Blockchain.

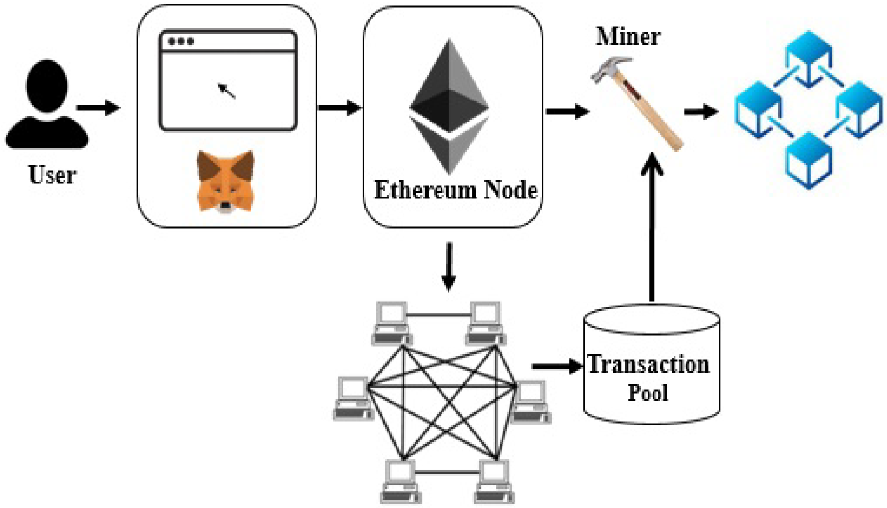


Figure (1): Blockchain operation principle and transaction validation.

Particularly a private Ethereum setup. Users propose transactions to the Ethereum network pool of other transactions, which other miners validate. Miners pick proposals from the pool, assemble them using a script into blocks, which they hash and then, hoping to do this correctly, solve computationally intensive mathematical problems under certain circumstances. This procedure protects the network from hacking or faking of the user identity. According to Ethereum's propaganda, mining on the Ethereum network does for us is ‘securing the network by creating, verifying, publishing, and propagating blocks' (Kushwaha, et al., 2022).

2.3 Blockchain Network Types and Consensus Mechanisms

2.3.1 Permissioned vs. Permissionless Blockchain Networks

Blockchain technology solves the trust problem while introducing a new layer of functionality– the ability to store data and transactions securely, transparently, and efficiently using a distributed network. Two broad paradigms have emerged in this space: permissioned and permissionless networks. Each paradigm has a different application that presents advantages and disadvantages and finds application in different industries. The fundamental legal distinction in Blockchain networks lies between permissioned (also referred to as consortium) and permissionless networks. Permissioned networks are networks controlled centrally, where a company cannot join the network unless a participating institution gives them the ‘go ahead’ or key. In many instances, businesses must first apply to select institutions to be able to join a permissioned network. These institutions are not predefined but vary on a network-to-network basis, and they can be banks, designated exchanges/brokers, numerous national banks, etc. In contrast, permissionless networks, like Ethereum, bitcoin or Dash, require no permission, and anybody can participate. Although there are fundamental differences between the two networks, they have unique advantages and pose various issues (Alkhammash, 2022).

2.3.1.1 Permissionless Blockchain Networks

Public Blockchains allow transactions to be conducted on what is known as a ‘permissionless network’. In a permissionless network, the rules provide equal access to all parties, resulting in a decentralised system where anyone who abides by the network’s rules may vote on and verify the next piece of the economic ledger, referred to as a block, which is the namesake for the Bitcoin network on which it was developed. These so-called public Blockchains are transparent in that any network activity – such as a digital transaction – is visible to everyone. Nobody has more rights than any other pod on the network regarding the protocol. Transactions are validated through a process known as a consensus mechanism (Asad, et al., 2020).

Advantages:

- **Transparency:** Permissionless Blockchains are transparent: Every transaction and any changes in ownership are visible to everyone on the network, dramatically increasing participants’ responsibility and trust in one another.
- Decentralisation: These networks are natively distributed, meaning they are not centralised; no central authority governs them. This distributed character mitigates censorship and single points of failure.
- Accessibility: Permissionless Blockchains are open to all. It is in their nature. Permissionless Blockchains are open-ended, peer-to-peer collaboration systems unbound by any rules.

Disadvantages:

- **Scalability:** The most severe downfall of the permissionless Blockchain is scalability: it can be challenging to achieve high transaction throughput, which makes it inappropriate for specific applications with a high number of transactions to process.

- **Anonymity:** While these networks' anonymity might protect user privacy, it also enables bad actors, making it easier to commit fraud and other nefarious acts without getting caught.

2.3.1.2 Permissioned Blockchain Networks

Permissioned, or ‘private’, Blockchain networks are open only to those intentionally invited to join and manufacture the chain. This exclusivity omits the randomness inherent in the open-source version and vets the participants (usually through a central authority or consortium).

Advantages:

- **Privacy and Security:** ‘Uninformed’ users have limited to no access to the Blockchain, ensuring high privacy and security because transactions and computations are only visible to a small number of ‘informed’ permissioned parties. This high level of security is critical for many industries, which is why the ‘technology was initially developed’.
- **Efficiency:** These Blockchains are generally faster and more scalable regarding transaction throughput. Efficiency is essential for organisations that require many transactions to be performed quickly and effectively.
- **Scalability:** Permissioned Blockchains are purpose-built to interconnect an entire industry through federated ledgers. Solutions can be built from the ground up, specifically for a given industry, and networks can be adapted to suit bespoke needs. Scalability can vary by network.

Disadvantages:

- Centralisation: The Blockchain's decentralised philosophy could be compromised by centralised control by a single organisation or cartel. Moreover, it might lead to governmental or corporate failure sites.
- **Limited Access:** Access for a select number of people can impede innovation and broader adoption. If only a few people can access the network, progress can be hampered in speed and adoption.

This range of possible applications highlights the difference between permissionless (public) and permissioned (private/consortium) Blockchain networks. Permissionless Blockchain networks favour openness, transparency, and decentralisation, while permissioned networks privilege privacy, security, and customised solutions. There is some trade-off between these models; for instance, an application may desire openness and transparency but prefer a private network to safeguard privacy and security or because a permissioned solution may be better suited for the application's governing parameters. As the Blockchain economy develops, determining what degree or extent of permissiveness versus restrictiveness can unlock and drive the most valuable use across industries and applications will be the key to maximising this technology's potential (Arachchige, et al., 2023).

2.3.2 Comparing Consensus Mechanisms

In a Blockchain network, achieving consensus is paramount among network participants, and different algorithms can cater to diverse needs. Some of the most well-known consensus mechanisms are the following:

Proof of Work (PoW): is the heart of the Bitcoin Blockchain and a buzzphrase in crypto. Miners compete for the right to 'mine' blocks. Each miner fires up their computer and churns through a cryptographic puzzle. The first puzzle solved gets to go next, recording their results in a 'block' on the Blockchain. They earn a crypto reward for their efforts. PoW is famously secure but computationally demanding on our computers and consumes a staggering amount of energy.

Proof of Stake (PoS): Rather than involving calculation as in PoW, the system chooses validators because they have locked up an amount of cryptocurrency. That amount determines the odds of their being chosen, but validators are nonetheless chosen randomly. PoS is much more energy-efficient than PoW but requires holding cryptocurrency to participate.

Delegated Proof of Stake (DPoS): With DPoS, users vote for a handful of delegates who create the blocks and vouch for transactions. The delegates take turns in a round-robin fashion. DPoS is more centralised than PoS but offers speedier, more scalable performance because fewer participants exist.

Practical Byzantine Fault Tolerance (PBFT): Most voting nodes must agree on valid transactions. In practical Byzantine Fault Tolerance (pBFT), a consensus algorithm, distributed systems can reach an agreement even if some nodes in the network are broken or malicious. Advantages of pBFT include Byzantine fault tolerance of up to one-third of nodes, a shorter amount of time for transaction finality without multiple confirmations until they are written to the Blockchain, and a Proof-of-Stake consensus protocol where all nodes participate in processing transactions unlike Bitcoin's Proof-of-Work design, which favours faster nodes. The disadvantages of pBFT include high communication overhead, which limits it to smaller networks for scaling purposes, and high susceptibility to Sybil attacks if a single entity can control several nodes.

Proof of Authority (PoA): PoA operates staked validators–entities chosen for their identity and reputation rather than because of computing power or quantity of cryptocurrency stakes. This renders the PoA ideal for permissioned or private chains with strict controls over validators. PoA is quick to achieve consensus and even faster than PoS, making it great for enterprise applications or IoT devices. The validators operate automated, closed-loop software to approve transactions and extend the chain without human intervention.

However, PoA networks fire a warning shot across the bow of crypto purists, as the validators could be a majority of one entity with a consortium of validators. Most PoA networks employ ten or more validators and have stringent vetting processes.

Every consensus algorithm has pros and cons: PoW is the most secure consensus algorithm but consumes vast energy. PoS is more efficient than PoW but also requires some form of staking. DPoS can achieve breakneck transaction speeds but is inherently more centralised since the validation nodes are elected. For use cases where all the participants can be fully trusted, such as enterprise solutions, PBFT is a great option, as it, too, has breakneck transaction speeds. PoA offers the best of both PoW and PoS by being very efficient – a vital aspect of any Blockchain due to the mining process. However, users should also keep in mind the degree of trust required. The energy problem—what effect does this consensus method have on the environment—is another essential factor to consider.

The proposed novel BCoT architecture consists of an interlinked network of Ethereum-based Blockchain. The deployment of the Ethereum Blockchain is the foundation of the proposed architecture. Therefore, the selection of the running node of the Ethereum Blockchain is of some importance. There are two major implementations of the Ethereum Blockchain at present. Major implementation includes the private Blockchain implementation named Quorum and Go Ethereum client (usually called Geth).

Quorum is an enterprise distributed ledger and smart contracts platform built on the Ethereum Blockchain but upgraded to the original protocol. Overlaid on the Geth client base, it uses the PoA consensus protocol algorithm Raft. Meanwhile, Geth is one of the official clients of the Ethereum Blockchain, written in Go. It implements the full Ethereum node and supports numerous consensus protocols, including the PoA-based Clique algorithm.

The Go Ethereum (Geth) client is the most preferred client for the BCoT ecosystem, primarily because it is the most mature. Ethereum clients like Geth have matured more than its competitor Quorum because it was made first and has been through more development cycles. This makes it a more mature client. Furthermore, the PoA consensus protocol Geth uses is more resource-efficient in securing a Blockchain than computation-intensive PoW-based protocols such as the one used by Ethereum. Devices acting as signer nodes in any BCoT applications will be deployed under constrained resource settings, lacking dedicated GPUs or extensive resource computation considerations. Hence, with the lack of technical resources available at the signer nodes, Geth becomes a prime candidate as its consensus algorithm enables distributed transactions to be committed with a significantly lower level of computational requirement at the participating signer nodes.

The Geth client is downloaded on all nodes, forming part of the Blockchain of Things ecosystem, and is used to deploy the Ethereum Blockchain nodes. Geth includes the core tools and functionality required to set up a full Ethereum node, including the Clique PoA consensus protocol and the deployment of the smart contract binaries on all the nodes forming part of the ecosystem. Using Geth’s maturity, stability, and lightness features, coupled with the Ethereum client’s PoA-based Clique consensus protocol, the implementation leverages a secure, lightweight, and efficient Ethereum-based Blockchain more suitable to the proposed architecture requirements than others. Table (1) summarising the different consensus mechanisms:

Table (1): Different consensus mechanisms pros and cons.

Consensus Mechanism	Description	Pros	Cons
Proof of work (PoW)	Miners compete to solve a complex mathematical puzzle.	Very secure	Energy-intensive
Proof of stake (PoS)	Validators are randomly selected to add new blocks to the Blockchain.	More energy efficient than PoW	It is less secure than PoW
Delegated proof of stake (DPoS)	Users vote to elect a small number of validators.	More scalable than PoW and PoS	Less secure than PoW and PoS
Proof of authority (PoA)	Validators are pre-approved by the network administrator.	Very scalable	Less secure than PoW, PoS, and DPoS

2.4 Blockchain Platforms and Off-Chain Solutions

2.4.1 Blockchain Platforms

2.4.1.1 Ethereum Platform

Ethereum – the first such decentralised Blockchain service, backed by a cryptocurrency of the same name – was the first to allow the creation and deployment of dApps or software apps that could execute entirely on the Blockchain. The native currency of Ethereum is Ether (ETH), which is used to pay for computational power or transaction fees to process its Blockchain. Ethereum also included a system for smart contracts: contractual arrangements that are not legally binding by themselves but programmed directly into the computer code. At the heart of the Ethereum Blockchain is the Ethereum Virtual Machine (EVM), which is the deployed execution environment for smart contracts on the network (Chen, et al., 2021). The EVM acts as the virtual environment that can consistently and securely execute smart contract code across all nodes in the network. It provides an abstraction of the layer between the executing code and the Ethereum nodes, and the Turing completeness of the EVM provides a way for a developer to build custom smart contracts and dApps without needing to produce the code from scratch. Ethereum supports the concept of being operated in a private or permissioned mode, where the Blockchain will be accessible only by a set of nodes (regulated by a central body) isolated from the public network. Such a permissioned setup can support specific use cases where there is a need for access control and additional privacy.

Developers write smart contracts for the Ethereum ecosystem in Solidity, a statically typed, contract-oriented programming language. Loosely based on a language called C++, Solidity borrows from its influencer in the form of inheritance and user-defined data types, allowing it to build on the library of existing structures and methods that other languages traditionally offer. In addition, Solidity contracts are ‘compiled’ into bytecode that the EVM can execute on every node in the Ethereum network in precisely the same way – executing the logic of the contract on every node in the system (Chen, et al., 2019).

The life cycle of a transaction on a PoA Ethereum Blockchain, as shown in Figure (2), starts when a user submits a transaction to the network. The transaction is sent to a pre-defined set of validator nodes that handle transaction validation and finalisation. A validator node will execute the request against their local copy of the Blockchain state (the rest of the network still operates similarly). For instance, it will check that the user has funds waiting to be sent, that the transaction is formatted correctly, and that any smart contract code the user wants to run is valid (including all the proper checks). After that, if the validator finds that the transaction is valid, it will create a new block containing that transaction (continuing the Blockchain data structure) and then send out that newly created block to all the other validators. The other validators will execute that block and its transactions. Once they have done so and agreed on the block validity, it will be finalised and added to the Blockchain – the data structure is updated along with all its included transactions. The Blockchain state has now also been updated.

PoA has a transaction finality much faster than PoW for two reasons, primarily due to the lack of significant energy expenditure miners must put into mine blocks. First, a transaction will typically be finalised in a few seconds after reaching the required validator agreement. However, this assumption already depends on the honest behaviour of its trusted validator entities. If a large majority of entities decided to collaborate to censor or reverse transactions, this would cause a breach of network security.

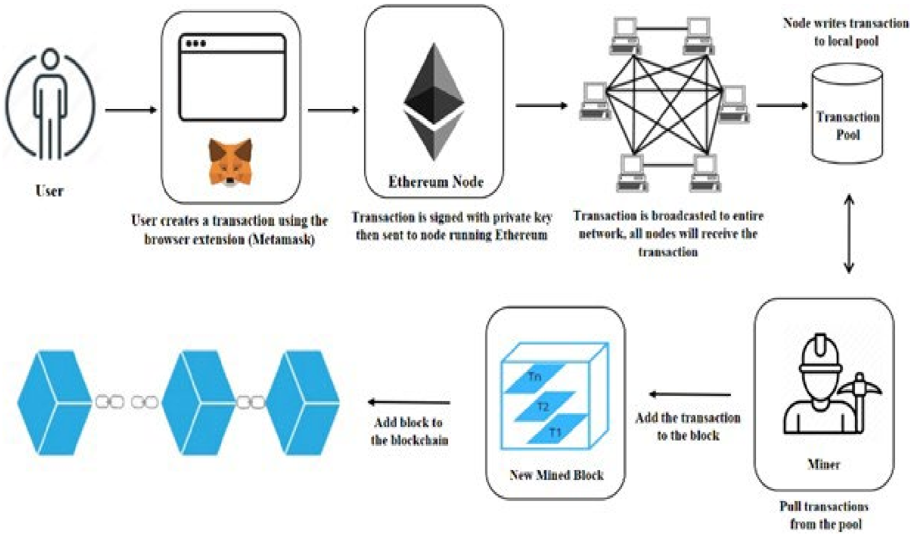

User
User creates a transaction using the browser extension (Metamask)
Ethereum Node
Transaction is signed with private key then sent to node running Ethereum
Transaction is broadcasted to entire network, all nodes will receive the transaction
Node writes transaction to local pool
Transaction Pool
Miner
Pull transactions from the pool
Add the transaction to the block
Tn
T2
T1
New Mined Block
Add block to the blockchain

Figure (2): Transaction block validation and addition flow.

However, the risk of centralisation also exists as most validator nodes could be controlled by one entity, which could interfere with the consensus protocol. Therefore, PoA networks tend to have more validator nodes than PoW networks and are usually extremely strict in their vetting process to ensure they authorise the right people. By striking a balance among the trade-offs between decentralisation and efficiency, PoA thus delivers a viable, secure, and reliable consensus mechanism for many Blockchain applications, particularly those involving decentralised IoT devices and full Ethereum nodes (Asad, et al., 2020). Deploying an Ethereum-based Blockchain for the proposed BCoT ecosystem requires carefully evaluating the available options. Regarding Ethereum implementations, two main choices stand out: Quorum and Go Ethereum (Geth).

After thorough consideration, the decision has been made to utilise the Geth client to implement the BCoT's ecosystem. This choice is primarily driven by the maturity and development stage of the two options. Go Ethereum is an older and more established Ethereum client compared to the Quorum implementation, which gives it an advantage in terms of stability and feature set. Additionally, the Clique PoA consensus protocol Geth uses is considered more lightweight and suitable for the resource-constrained devices in the proposed BCoT ecosystem (Melissari, et al., 2021).

Unlike protocols based on PoW, Clique PoA does not require dedicated GPU processing, making it a better fit for the targeted devices that will likely rely on CPU-based execution. The Geth client will be installed on all the Blockchain of Things ecosystem nodes to deploy the Ethereum Blockchain nodes. Geth provides the necessary tools and functionality to develop a full Ethereum node, including the desired PoA consensus protocol (Clique) and the deployment of smart contracts across the different nodes. By leveraging the mature and well-established Geth client and its Clique PoA consensus mechanism, BCoT's ecosystem can benefit from a secure, efficient, and resource-friendly Ethereum-based Blockchain solution that meets the specific requirements of the proposed architecture (Zhao, et al., 2023).

2.4.1.2 IOTA Platform

The IoT ecosystem has seen the rise of IOTA, a ground-breaking distributed ledger technology that utilises a unique data structure called the Tangle. The Tangle is a DAG that avoids cycles or loops, enabling numerous applications with secured and verified data. IOTA's Tangle ensures data integrity and security, particularly in healthcare, where it can safeguard data flows from remote sensors and create immutable records for clinical trials. The MAM protocol facilitates secure data exchange among stakeholders. Additionally, IOTA's Tangle offers a unified identity for IoT devices, streamlining device management and enhancing security across industries. IOTA enables decentralised energy generation and distribution in the energy sector through machine-to-machine interactions, such as intelligent charging for electric vehicles. The mobility and automotive industries can benefit from IOTA's "digital twin" technology, enabling use-based insurance models and peer-to-peer vehicle rental services. IOTA's Tangle also provides a secure and transparent platform for government services like voting and medical record management, mitigating identity theft and fraud risks. Recognised as a "Better Technology Tomorrow" by TechJury, IOTA's Tangle has versatile applications across industries that require data integrity, security, and decentralised operations (Chen, et al., 2021).

2.4.1.3 Hyperledger Fabric Platform

Hyperledger Fabric, an open-source, enterprise-grade DLT software development framework, stands out for its sophisticated cryptography, scalability, and modularity. It was initially developed by IBM and later released as open-source, making it a powerful tool for building private Blockchain applications. Its unique features make it an ideal choice for many use cases.

Hyperledger Fabric's practical applications are evident in supply chain management. It tracks goods or services from their source to the end consumer by providing transparency and traceability. This level of detail can help multinational companies combat fraud, enhance efficiency and accountability, and improve product quality.

Hyper ledger Fabric provides a secure identity management system, which can be crucial when identities must be verified and authenticated, especially in medical fields like hospitals, banking, and administrative purposes where centralised records are kept. The financial services sector can use it to provide a secure and transparent platform for financial transactions that saves money, reduces fraud, checks for errors, and speeds up payment times. It will also provide a platform for developing newer financial products. It also supports micro-transactions between IoT devices, among other uses, to provide more citizen services like voting, sharing of medical records or others, essentially accessing available government services without the need to provide identity with a risk of theft or fraud. Likewise, it allows building a supply chain network that includes manufacturers, suppliers, and distributors to make the manufacturing of products more efficient, cheaper, and transparent (Shahbazi & Byun, 2021).

2.4.1.4 Review of a suitable Blockchain platform

Choosing the right platform is an important design decision that can dramatically impact a Blockchain project's potential success. To deliver Blockchain solutions to resource-constrained, low-power, low-resource hardware such as a Raspberry Pi, the Ethereum Blockchain offers significant advantages to similarly scalable Blockchain solutions such as Hyperledger Fabric or IOTA. Ethereum offers a more mature platform with a broader developer community and an established ecosystem. It is the most suitable option for decentralised applications optimised for low-power, low-resource hardware (Scheid, et al., 2022) (Lu, et al., 2021) (Muradi & Chiam, 2022).

Why use Ethereum for RPi4 networks?

The Power of Smart Contracts: Beyond its solid cryptography foundations, the other significant advantage of Ethereum is its advanced smart contract architecture. The EVM has a proven, secure engine for executing smart contracts, an essential requirement of many Blockchain applications. The built-in toolchain (all part of the EVM for free) is available, and the Raspberry Pi is sufficiently robust to allow low-latency smart contract execution.

It also supports a wide range of languages for developing dApps. It is also easier to assemble a development team for Ethereum-related development, given the highly active, supportive developer community in this field.

A Thriving Ecosystem and Developer Support: The Ethereum ecosystem is mature and large, with many libraries, tools, and an active developer community. Working with a Blockchain network is more accessible if that network has ecosystems similar to what Ethereum offers, with many tutorials, mature libraries, and a vibrant part of the Blockchain developer network that can help solve problems and debug.

This supportive material – tutorials and friendly disclosure communities – can dramatically decrease the entry barrier to Blockchain technology. This democratisation of knowledge and skills enables a wide variety of people from diverse cultures and classes in the world to learn Blockchain technology and participate in the construction of the new technological system, thus leading to the innovation and wide adoption of Blockchain technology.

PoA Consensus Algorithm: A suitable PoA consensus algorithm can be implemented in Ethereum, a robust and well-documented open-source solution. For permissioned Blockchain networks, such as an RPi4 network, the idea behind this algorithm is to eliminate the concept of a distributed consensus algorithm. Instead, the network signers — the equivalent of miners for a PoW network—will be a known and trusted set of validators, usually verified by semi-trusted third-party organisations.

Energy Efficiency and Scalability: Although Tangle was designed with many novel features, its virtues as a consensus mechanism might be better suited for more powerful resource-rich devices such as laptops and workstations than the Raspberry Pi. Meanwhile, Ethereum is also transitioning to a PoA consensus mechanism. It remains to be seen whether this transition results in significant savings in energy usage and makes the protocol more suitable for low-power, resource-constrained devices such as the RPi4. Moreover, much-anticipated improvements have been incorporated into the roadmap for the Ethereum protocol. Some examples are sharding and layer-2 solutions that might significantly improve performance and scalability, potentially benefiting RPi4.

2.4.2 Off-Chain Storage: IPFS

IPFS is a peer-to-peer hypermedia protocol and a distributed file system that aims to ‘solve’ the shortcomings of the design of the current centralised web. IPFS skirts the issue of storing and moving files across a distributed network of billions of users differently. Fundamentally, it tries to solve all the issues plaguing the first large-scale information network built on a centralised architecture. Centralised architecture had its roots in dealing with engineering realities. However, it later resulted in duplication and incoherence of data flow – problems that led to the birth of distributed processing and storage as a solution. A distributed file store with content-addressable storage allows for a system's network where content acts as identity in IPFS, which makes it ‘unforgettable’. It is this identity that becomes one of IPFS’s strengths.

IPFS, with its unique off-chain storage capabilities, introduces a new paradigm in data storage. Let us delve into its critical aspects:

Storage and replication: IPFS ensures the safety of your data by allowing files to be replicated across a network of all the node operators. This peer-to-peer storage approach, as opposed to individual server storage, significantly enhances data security. The files are stored by breaking them into smaller pieces and distributing them across all available nodes, making it a safer data storage option.

Content-Addressed Storage: Instead of storing files under unique directories or having one IP address (URL) point to different content, IPFS creates content hashes (identifiers) directly tied to the file. This inherent content-addressing function means that ‘links refer directly to content itself, independent of paths or URLs as we currently know them. Since links, in this case, reference the content rather than where it is stored, they are permanent and immutable as long as it is still available. This architecture underpins the decentralised verification of content integrity and even data deduplication: IPFS can refer users to the exact copy of a file regardless of where other copies exist.

Bandwidth Optimisation: IPFS uses parallelised retrieval, which means we pull pieces of a file from many different nodes simultaneously. This can drastically save bandwidth, as people all over the planet can share backed data at high-traffic rates, and no one has to re-upload anyone else’s bits.

Resilience and data security: By splitting the data across many nodes, IPFS makes the file resilient—if one node dies, others will have identical copies of the data and can still serve the data. It is available. Cryptographic, one-way integrity checks (ensuring data has not been tampered with or changed back to past copies) can also be inserted.

Off-Chain Storage: Using IPFS, files can be stored off-chain: the transaction can record information about the files in the form of immutable permanent links known as Content Identifiers (CIDs), and using CIDs, we can determine if the file has changed or remains the same. This allows nodes to store data off-chain while maintaining a permanent recording that can include provenance and timestamps, and it guarantees the integrity and security of the content without storing the data on-chain. Providing CIDs and a hash table that records when they ‘change hands’ empowers anyone to build and share on the decentralised web in new ways, free from the shackles of the limited and centralised on-chain storage facilities inherent in Blockchain technology.

The decentralised storage, content-addressing, bandwidth optimisation, robustness, and off-chain storage capabilities of IPFS might all be utilised in such an iteration. The foundation for all online human interaction and activity might be stored and accessed through a leaner, more secure, and far more scalable infrastructure.

As described above, IPFS is compatible with Blockchain technology. It offers a highly scalable and cost-effective off-chain storage solution by decentralising file storage and retrieval, ensuring the creation of decentralised applications with potentially extensive data requirements (Confais, et al., 2017) (Huang, et al., 2020).

2.4.2.1 Transaction Flow for Ethereum Blockchain and IPFS Integration

The synergy between the Ethereum Blockchain and the IPFS, a peer-to-peer distributed file system, allows for the creation, storage, and retrieval of large files on-chain, along with our mechanism to allow for robust smart contracts based on verifiable on-chain self-executing agreements and secure hardened cryptography.

This vortex of smart contracts – a scalable, affordable, off-chain storage solution for decentralised applications – is made possible by the coordinated effort of these two avant-garde technologies. Let us look at the footwork:

1. **Upload to IPFS**

   The trip begins with uploading the requested file or content to the IPFS system, through the IPFS API, or with IPFS’s user-friendly desktop application. Once uploaded, the file is cut into pieces or hashes, duplicated, and dispersed in millions of nodes wherever the network is occupied.

2. **Create the IPFS Hash**

   When a successful upload is achieved, IPFS returns a ‘content hash’ for the file, which can then be accessed and retrieved by that hash on the network.

3. **Create an Ethereum Smart Contract**

   It functions as the interface between and connects Ethereum smart contracts to the IPFS, a distributed file system that can store and host digital assets. The smart contract is deployed on the Ethereum Blockchain to manage IPFS uploads.

4. **Store the IPFS Hash in the Smart Contract**

   Now, the IPFS hash of the file (essentially identifying the file's location on IPFS) is stored in the Ethereum smart contract in the variable mentioned. This is a crucial step as it connects the file on IPFS and the smart contract on the Ethereum Blockchain.

5. **Interact with the Smart Contract**

   From there, users could ask the smart contract to deliver the file stored in IPFS. This could all be done conveniently via a web3js-enabled browser. A more elegant solution is to use a dApp.

6. **Download via IPFS**

   The file retrieval is initiated after a user obtains the IPFS hash (a file’s unique identifier) from the Ethereum smart contract. The obtained hash can be used to download and then reconstruct the file from the decentralised IPFS network.

7. **Access the File**

   Once that file is identified and located by the IPFS network, it can be downloaded and viewed by the user at the push of a button, granting direct access to decentralised storage and retrieval.

This integration of Ethereum and IPFS is a monumental step in decentralised technologies as it allows for the safe, traceable, and efficient storage and retrieval of data. By merging the strengths of each technology, developers can now create decentralised applications that radically change how data and content are handled.

2.5 Blockchain Integration with Emerging Technologies

2.5.1 Integrating Blockchain of Things (BCoT) with AI

Several related works have tried integrating BCoT with AI and building a secure and intelligent system. For instance, Zhang et al. proposed the architecture of an MBCoT to build a safe, traceable, and decentralised IMS. More emphasis has been put on structuring a data and knowledge-driven digital twin-manufacturing cell using MBCoT to increase operational efficiency and accuracy. Ultimately, they also provided implementation details of the MBCoT prototype system and application cases to show how practical and effective IMS-based MBCoT is. However, at least several limitations are mentioned. IMS is more of a concept than a mature system, with vague definitions and participants. Integrating Blockchain with the IIoT is still immature; its complexity may result in a problem of managing massive data, information, and knowledge flows on the one hand and concerns of privacy and security on the other hand. The prototype demonstrated the feasibility, yet applying and scaling MBCoT in varied manufacturing ecosystems may still be challenging. What this study reveals are some drawbacks of IIoT-based centralised IMS. The authors wonder if Blockchain technology may help to address these problems, and they also point out the persisting complexities and at least one challenge of real-world deployment of such technology and when it is integrated within the industry (Zhang, et al., 2020).

One very recent state-of-the-art review presents how Blockchain can improve the security and efficiency of eHealth systems (Almalki, 2024). It also analyses the integration of IoT, fog, cloud, and Blockchain integration to securely manage information and data in health care. Finally, it outlines the methodology for integrating Blockchain and IoT to provide a secure and reliable platform for health record monitoring. The technical procedure also provides secure and reliable health record storage based on smart contracts for managing the user/device request in a private Ethereum-based infrastructure (Alam, et al., 2023).

Another paper presents how Blockchain technology and IoT can be integrated using predictive sensory and contextual awareness with dynamic responses to secure the health record. This article suggests how to improve the security of health record storage using smart contracts for managing user/device requests based on secure and reliable health record storage using smart contracts (Wenhua, et al., 2023). Moreover, another paper explains the security vulnerabilities with the application of Blockchain in health services using IoT-driven healthcare services for smart cities. The aim is to show how to provide enhanced electronic health record (EHR) privacy and security through innovative encryption techniques (Xue, et al., 2022). Another comprehensive survey paper reviews Blockchain-based resource management solutions for edge computing environments. The applicability of AI and machine learning techniques for resource allocation in Blockchain-based edge computing systems is also presented. (Badidi, 2022).

In addition, the integration of edge computing, IoT devices and Blockchain for intelligent city applications was examined. This article presents how AI and cognitive computing techniques can be leveraged to compute data and make decisions at edge nodes. The edge AI and Blockchain technologies application is also presented for processing a large amount of data locally and enabling real-time applications (Singh, et al., 2020).

Furthermore, a secure infrastructure of IoT-oriented deep learning is proposed to build a smart city by adopting Blockchain, which could provide security and integrity to the data. For this purpose, an additional deep learning model is proposed to process the intelligent data and make decisions. Another study introduces a BCoT architecture combining edge computing, AL, and IoT devices for gathering and analysing environmental data by adopting an AI engine to predict and share results over a public Blockchain platform. According to the authors' recommendation, it has been tested as a real-life parasite origin tracing service use case. It demonstrates an accuracy of 95% for COVID-19 disease that spreads out in sewage water. While maintaining data integrity through Blockchain, one drawback of this system is the possibility of false or fabricated sensor data with which some inaccurate or untrue readings may contaminate the acquisition of trusted data (Alrubei, et al., 2022).

2.5.2 Blockchain and IoT Integration

The inherent design limitations of IoT devices can also make them appear particularly vulnerable to adversaries. IoT devices are often designed with lax security, low processing power, small storage, and computing capabilities and are notorious for handling sensitive, privacy-critical data. This makes them an ideal target for attackers seeking to exploit them for illicit purposes and access the vast amounts of data they process. The hidden vulnerabilities of IoT devices can be thus leveraged by Blockchain technology and further ML advancements that would not only add value in an IoT paradigm but also ensure trusted, secure quality of data and latency and add more transparency to the systemic functioning. Furthermore, the IoT could be combined with cloud computing infrastructure to scale up systems' processing and storage capacity. Another salient feature of Blockchain is that there is no centralised authority. Instead, documents and transactions are recorded in an identical copy on each distributed server throughout the network, so the data verification is conducted in a consensus-predefined and through smart contracts (AlSadawi, et al., 2021). Blockchain also provides the next level of connectivity for IoT units, which can work directly without the involvement of any central server. This means duplication of data and speedier message transmission from one unit to another in a designated Blockchain. Additionally, Blockchain ensures that this newly generated data is validated and maintains the exact authenticity for each connected unit. In other words, IoT data becomes more reliable with Blockchain. Security is automatically ensured in this scenario since cryptography is an integral part of Blockchain design, and the use of hashing algorithms to interlink the chains is part of the basic functioning of this technology. Its re-emergence with Blockchain applications for IoT is propelled by IBM's 'Autonomous decentralised peer-to-peer telemetry' (ADEPT) platform, the first decentralised approach to deliver improved scalability and security (Windley, 2015).

Some recent studies have implemented Blockchain and IoT integration, discussing different solutions and approaches for various situations (Aich, et al., 2019) (AlSadawi, et al., 2021) (Shammar, et al., 2021) (Dai, et al., 2019) (Conoscenti, et al., 2016) (Dorri, et al., 2016) (Atlam, et al., 2018). For example, a DAO (Decentralized Autonomous Organisation) could be established on the Ethereum network, using smart contracts built in solidity language to automate the organisation's operation and decision-making for a team of people working autonomously outside of a corporate structure (Jentzsch, 2016). Xiao et al. proposed a new Blockchain-based IoT system architecture for automating and allocating IoT tasks and resources in home, factory, and hospital environments. The proposed architecture consists of a device layer and a distributed agent controller. The distributed agent controller intermediates between the device layer and the Blockchain. Blockchain is embedded in the middle layer, guaranteeing transaction information security

(Xiao, et al., 2020). In contrast, Sharma et al. used a three-layer distributed cloud model based on fog computing to govern the IoT's raw data stream at the edge and the cloud layer (Sharma, et al., 2018). Meanwhile, Moinet et al. proposed a secure protocol and decentralised model of Blockchain cryptographic keys and depositories of reliable data for peer-to-peer wireless mesh networks, each with components for validating data belonging to the rest of the network peers (Moinet, et al., 2017).

To prove the security and scalability of a Blockchain-based IoT system, a proof-of-concept developed in the form of a private Ethereum Blockchain and utilised an RPi to capture, store, and consume the data generated by the IoT devices and sensors in a secure, authenticated, and distributed manner. The actual encrypted data is finally pushed to the IPFS or Swarm file system, while the identity of this data is still authenticated and encrypted with the cryptographic critical identity (PKI). After all keys have been registered, they will be locked and stored on an RPi, where the Trusted Platform Module (TPM) provides robust key management, encryption, and disk encryption (Ramesh, et al., 2020).

Accordingly, Fernando and colleagues tested IoT devices using Blockchain technology, integrating low-cost RPi minicomputer devices with the Ethereum platform and applying them to the pharmaceutical sector, they achieved satisfactory results (Fernando, et al., 2019). Furthermore, an IoT system based on Blockchain technology was developed, which relies on a mobile app to identify systems such as orphanages using volunteers' smartphones. The system collects on-chain and off-chain data that are generated by networked RPi sensors to allow service providers, donors and rice suppliers in the network to track system activities, such as storing rice of financial transactions, thereby reducing the manipulation of relevant interactions using smart contracts, and improving system transparency (Junfithrana, et al., 2018).

In contrast, A Blockchain emergency service was brought into a smart home infrastructure for access control of untrusted public utilities and smart home IoT devices (Tantidham & Aung, 2019). The system consists of an RPi to collect readings from in-home sensors and of the Ethereum-based platform, connected to a web application to monitor the activity – and open to home users as well as with home service provider employees – and of the IPFS database to process files produced by the smart home, in principle making it impossible for a DDoS attack to occur. A web interface based on the Ethereum Blockchain to enable quick and effective renewable energy transactions is described as ‘Near-real-time, consumer-to-consumer energy transactions are enabled without a centralised authority (Park, et al., 2019). Devi et al. described a design architecture for satellite observation relying on IoT and Blockchain to envision a novel architectural structure enhancing the security and transparency of the data using consensus algorithms in forecasting different satellite performance metrics (Devi, et al., 2019).

In the past decade, Blockchain technology has rapidly gained attention and become relevant in many fields, notably in cryptocurrencies; although in its early stage of development (as depicted by the tech being featured in the Gartner Hype Cycle), it is essential to understand the path to maturity and evolution of the technology. The Gartner Hype Cycle is a pictorial representation of the development, maturity, acceptance and benefit of a modern technology or application through five phases, namely, the technology trigger, the peak of inflated expectations, a trough of disillusionment, and the slope of enlightenment and finally, plateau of productivity growth.

As Blockchain progresses through the cycle, we may see applications reaching the plateau of productivity growth realised relatively quickly. At the same time, the Hype Cycle is not just a predictive tool but a crucial guide that indicates the time expected before reaching the peak of productivity growth. According to the Gartner Hype Cycle for 2021, Blockchain technology is the bubbliest, most exciting of the 100 hype cycles the company evaluated, as shown in Figure (3).

Technologists and other observers can learn to observe emerging technologies with analytical eyes so that expectations are tempered and kept in line with reasonable expectations of emerging technology over time. This is what the Hype Cycle does. It provides a roadmap for the evolution of newer technologies, helping all stakeholders plan their investments, programmes, and press announcements in line with what they expect might happen with Blockchain technology as it goes from the current hype of inflated expectations to the more reasoned analysis of the slope of enlightenment and, finally, the plateau of productivity (Markus & Buijs., 2022).

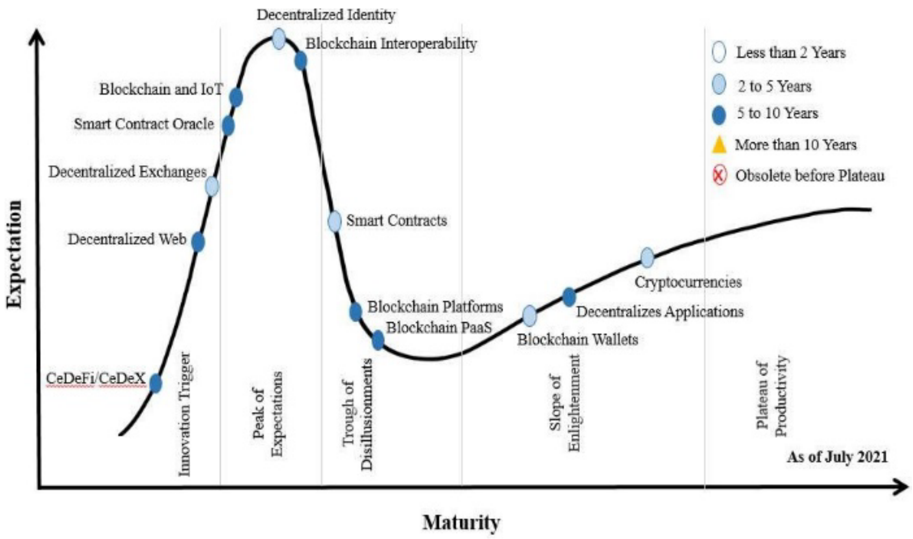


Figure (3): Blockchain Gartner Hype Cycle for 2021.

As a convergence of disruptive technologies, IoT and Blockchain exhibit high compatibility of two technologically mature platforms without any visible complexities to combine the two digitalised approaches. These novel technological platforms are not just expected but poised to address emerging global industrial and social challenges in a wide range of industries with tremendous growth potential. That text is mainly based on Gartner's published survey report in 2019, where over 500 US companies were surveyed regarding their adoption of IoT and Blockchain over the past nine years of hi-tech disruption and as a demonstration that most of the respondents have adopted Blockchain alongside IoT and satisfied with the most appropriate platform for their digital transformation and is expanding at a faster pace as expected. The Cycle is not a scientific method for the Tech Readiness Level (TRL) but only a conceptual and perceptual outline of how the cycle demonstrates the perception of the digital cycle of the technological rate of change over time (Markus & Buijs., 2022).

2.5.3 Integration of Blockchain and Cyber-Physical Systems

A CPS is another IoT idea, but rather than being a 'thing', it is more of an architectural form. IoT is simply a collection of intelligent sensors and devices linked to the Internet, but a CPS architecture incorporates remote processing, networking, control, and monitoring of intelligent sensors (Bhawana & Kumar., 2021). Therefore, the unique new possibilities of CPS arise from the unique and specific cyber-physical interactions, in other words. Big data technologies are changing the overall picture, leading to radically new and dire risks for the CPS of the emerging IoT and associated systems that need to be mitigated to preserve their fantastic advantages. On the other hand, many recent problems arising from additional complications, limitations and dynamics of CPS can neither be solved nor the full potential of the latest technologies be realised with the previous centralised data management approach – too many aspects are incomparable to the traditional model. What is needed is a smooth, decentralised data approach in line with the unique characteristics of these new systems. With its potential to transform the trust infrastructure of CPSs, Blockchain offers a reassuring solution to these challenges. Recently, it became clear that Blockchain solutions might be one of the most effective ways to address the abovementioned problems. For instance, by now, plenty of applications of Blockchain technology for CPSs exist – in medicine, transport, and cybersecurity. In particular, a recent review paper by Zhao et al. provides an excellent, condensed snapshot of the most recent developments in combining Blockchain with CPS to enrich its different components: providing data integrity for offline storage to protecting critical operations from real-time cyberattacks. They also show that research in this area is still in its infancy (Zhao, et al., 2021).

In addition, Blockchain has recently been applied to managing a CPL data collection on Ethereum Blockchain. The laboratory data is stored in the Blockchain; next, it is processed, analysed, and available in a fully transparent, traceable, and secure way. This novel technique allows the data to be streamed and broadcast in a decentralised way across peers with restricted visibility to the network while at the same time ensuring that the privacy of students' data sets and reports is not compromised (Al-Zoubi, et al., 2022).

2.6 IoT, Big Data, and Blockchain Synergy

2.6.1 Standard IoT Ecosystem

The fundamental structure of the IoT essentially comprises three layers, including a physical or perception layer, a network layer, and an application layer; as shown in Figure (4), the physical layer that composes the primary device in IOT architecture is physical devices or hardware sensors process information about the IoT physical world, a physical device will communicate with other devices and send data to receive the required information. Communications protocols and messaging services such as RFID, MQTT, AMQP, WSN, Bluetooth (Bluetooth and ZigBee), Wi-Fi, Routers, Switches and Firewalls are delivered and shared across the PAN, PLC, the WPAN, and within the WPAN BAN and finally PAN itself.

The network layer is a gateway device line for designing communication with other sensing network nodes and application platforms such as desktops, remote-control devices, smartphones, and other IoT equipment. It is also connected to the cloud server to save and analyse previously received data.

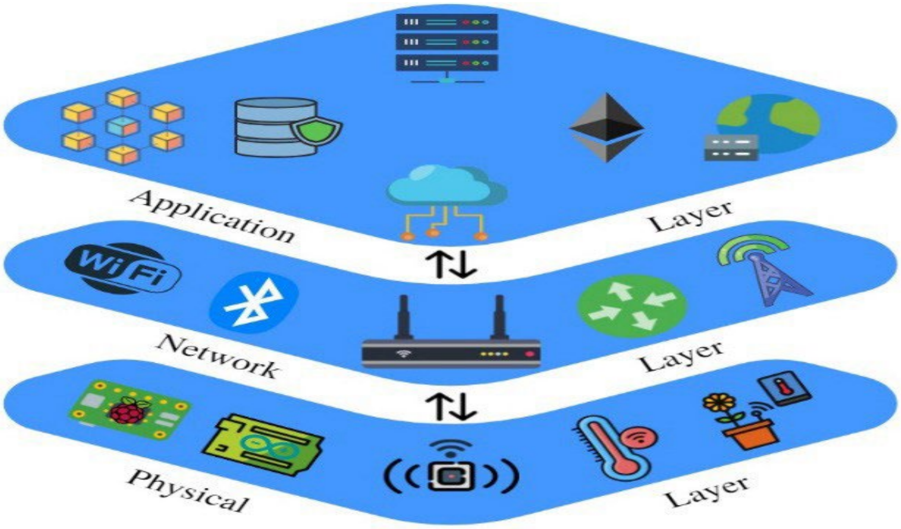


Figure (4): Basic three-layered IoT architecture.

The network layer lies in between the physical layer and the application layer. It adds gateway functions to facilitate direct communications from the physical layer to the application layer. For example, SDN can control actuators from desktops, smartphones, and other IoT hardware. It directly connects to the cloud servers, or the Internet in general, where the data from the physical layer is waiting for further analysis or stored for later use. This layer relies on protocols and technologies enhancing communication such as routing, addressing, messaging, publish/subscribing, rate and flow control, reliability, and QoS. Advanced 5G is high-speed for connecting sensors or smart devices to SDN, while IPv6 provides ample address space for the trillions of devices awaiting IP-enabled (Darwish, 2018).

The application layer provides end-users with numerous applications and services in health care, manufacturing (Industrial Internet), smart cities, logistics, retail, environmental monitoring, public safety, etc. It provides various functions, including QoS, device management, function processing (business process management), authorisation, key authentication and management, trust and reputation management, and identity management. The application layer enables waiting for consumer applications to provide personalised applications based on the data and application capabilities of the layers below so that different types of end-users can offer valuable services and applications for end-users in various fields (Darwish, 2018).

2.6.2 The IoT, Big Data and Blockchain Convergence

The exponential growth of the Internet of Things (IoT) has been a primary catalyst for the development of Industry 4.0 and the operation of the so-called Factory of the Future (FoF). Smart manufacturing relies entirely on adopting the Industrial Internet of Things (IIoT). Since the emergence of Industry 4.0, security and privacy concerns have been paramount. Unfortunately, the fragmentation and loss of meaningful industry IIoT data across Industry 4.0 operations with multisource data silos have become a persistent challenge in FoF operations. This is partly due to historical data management approaches developed from enterprise data management (EDM), which cannot effectively address the multisource and massive data heterogeneity problems that derive from the IoT environment, particularly in data integration and data analytics (Garcia-Loro, et al., 2021).

Blockchain is a complicated ecosystem, but its values are indisputable: uniqueness, decentralisation, immutability, traceability, economies of scale, and its capacity to constantly build upon itself. As such, this emerging technology might represent a disruptive force in exchanging and distributing data. Blockchain might prove to be a technology of choice for creating trust in distributed systems without the need for a central authority. Unsurprisingly, it is widely expected to be a breakthrough in many domains, such as the IoT, and represent a promising solution for achieving secure, transparent, and efficient data governance (Zheng, et al., 2020).

The merger of Blockchain technology and the IoT is a new milestone for evolving complex connected systems. The number of IoT devices has been proliferating, as is the volume of IoT-related big data and applications. However, most IoT adopters are still using closed network systems, which are vulnerable to attacks and cannot ensure a uniform and effective handling and processing of IoT data. As a result, IoT-related big data may be tampered with by device owners, accessed by internal users without authorisation, or even stolen by external cyber-attacks. It is a challenging job to detect and prevent a data breach. Therefore, IoT data could lose trustworthiness. This highlights the urgent need for a secure, decentralised architecture to ensure IoT data integrity, horizontality, scalability, and immunity to potential vulnerabilities.

Due to these limitations, integrating Blockchain technology into the IoT could solve some of these problems, ultimately leading to a decentralised, transparent, immutable, and incorruptible database for data management. Being able to leverage the principles of Blockchain, such as distributed consensus mechanisms, cryptographic security and tamper-proof record-keeping, IoT-enabled applications and infrastructures can substantially benefit from more integrity in data, better traceability, and more confidence among the users. Moreover, the complementarity of IoT and Blockchain technologies paves the way for new applications and use cases that no company or individual could have envisioned before the consortium computing era. From supply chain optimisation and provenance tracking to smart cities and emerging business models such as decentralised autonomous organisations, the union of these technologies will have a disruptive impact on industry sectors and human resources. Indeed, in the future development of the IoT, Blockchain will become one of the most significant steps in solving the problems of data authorisation and integrity. It makes sense to combine the merits of both technologies and realise the cutting-edge applications of IoT, helping businesses achieve a more efficient digital transformation (Zhaofeng, et al., 2020). With IoT devices coming faster than ever, applications based on big data and big data are gaining more and more significance. In comparison, there is no good safeguard of the standardisation process of IoT data so far. If the owners of collected information on collecting devices give up the information from the collected data for unreliability or the collected data has been fabricated operation by an internal user or has been assaulted (hacked) by a third party, the data that has been modified after-effect will be challenging to process.

Zhaofeng et al. then presented a public service exposed by an Ethereum decentralised security-service chain for IoT Big Data – pseudo named BlockBDM. All data transactions and data management operations, including data creation, data dissemination, and data storage, will be operated by a distributed Blockchain smart contract. What is happening in the real world is the consumers' incentive scheme providing and paying for high-quality data input with cryptocurrency, and all the input data will be recorded safely on a distributed worldwide Blockchain, including input with cryptographic hash function, transaction in node and high-security block. User control was protected with digital rights management. In contrast, crypto data consumption was used as a crypto data-leakage solution to prevent the data from being leaked or accessed by others. Thus, an open and visible Blockchain on IoT's big data. Meanwhile, experiments prove that the above-decentralised credibility management model of IoT's big data is feasible, safe, and scalable (Zhaofeng, et al., 2020).

Integrating the IoT with the Blockchain brings many challenges, including computational power, storage capacity and resilience during power outages. One of the biggest problems is that a lot of computational power and storage capacity is required to write data into a block of the Blockchain. Moreover, transmitting data on the Blockchain is very costly in terms of computing power consumption and an undesirable latency, making real-time operations and analysis of IoT data difficult. As a solution for these problems, distributed node architectures and efficient cloud platforms have been proposed (Hang & Kim., 2019). Lee et al. proposed a distributed node system connected with a cloud platform mounted on NVMeOF to enable the end-to-end informed collection of data from IoT nodes. An IoT-Blockchain Ethereum system was created to use smart contracts of Blockchains to verify the source of the data and store them securely at the system's edge. It was tested based on the NVMeOF-SATA storage communication protocol using healthcare data throughput. NVMeOF combined with Blockchain has many benefits. Kumoscale creates a storage solution to collect data from IoT Blockchain cloud applications. Data from several types can be cleverly pushed out from the edge via NVMeOF using an out-of-band network over some shared CPU bandwidth, and it serves as a system of executing CPUs with specialised capabilities. In this way, the high efficiency of NVMeOF connected to the Blockchain to on-board and process data can provide data with high performance and low latency for Blockchain applications. Furthermore, NVMeOF, as the edge storage fabric, offers better transaction I/O performance than traditional Ethernet technologies, allowing faster data processing speeds. This solution will help address the existing challenges – computations, storage, and latency – for Blockchain applications on the IoT, which leads to efficient data management and analytics (Lee, et al., 2019).

Blockchain could present opportunities and challenges for IoT as well. In one study on the integration of Blockchain and IoT, Reyna et al. explored the main application domains where Blockchain can serve as a facilitator of the evolution of IoT systems and a potential enabler to achieve the goals of such systems. This study mainly investigated whether running Blockchain nodes directly on IoT devices is feasible, which might make Blockchain integration make sense. However, the benefits of Blockchain in IoT must be thoroughly analysed and carefully conducted. In addition, the research determined the prime industries where Blockchain technology can accompany the development of an IoT system by assessing the feasibility of utilising Blockchain nodes on IoT devices. Similarly, the existing platforms and applications have also been examined to obtain a deep insight into the synergy between Blockchain and the attached IoT technologies (Reyna, et al., 2018). Then, regulatory approval is demanded to integrate Blockchain and IoT into public services before it is widely used and adopted. It would accelerate the bonding between people, the government, and companies. The consent could expedite the integration of the IoT in mines and the dissemination of Blockchain apps. Nevertheless, there must be more tension between database security and the ease of connecting embedded devices. Therefore, it is essential to conduct disruptive research to guarantee the security and confidentiality required by some essential technologies that IoT and Blockchain are gradually adopting. One of the major concerns for Blockchain is its constant volatility, especially with cryptocurrencies, as some of its users exploit it (Reyna, et al., 2018) (Kamangar, et al., 2023).

Alam's research sought to enhance and integrate a significant data mining architecture to function using Ethereum Blockchain in smart cities. More than 75 billion connected nodes are worldwide, and most do not use Wi-Fi as their communication technology. These nodes are mainly produced for industrial applications, such as smart manufacturing factories and homes. One of the main motivations of smart cities is to produce new communications technologies, allowing information translated by different internet technologies to be transmitted from smart cities' infrastructures. A high quality of life for the city's citizens depends on smart city infrastructures. Significant data analytics impact on these infrastructures allows their development and utilisation in smart cities. Furthermore, big data can be used to mine data produced by IoT devices to enable further studies on understanding smart cities. Sensors extensively produce big data in a smart city. If well-designed, these data can have a considerable impact. It could enable a Blockchain-based framework using Ethereum for mining big data in smart cities to enhance data transmission and security in the heterogeneous environment (Alam, 2020).

Kamal et al. presented a complete learning kit as a training solution for students trying to understand more about the latest IoT and Blockchain technology advances. The complete learning kit is structured in three parts: 'Brain,' 'Muscle,' and 'Cloud '. The Brain component uses the RPi to interface with a cloud platform where the data are transferred between the Brain and the Cloud using Xojo software. Similarly, the Muscle component adds functionalities to the Brain to input large volumes of data into the system and uptake these data by transferring from the Brain to the Cloud via the cloud platform interacting with Xojo. Finally, the cloud component refers to data storage and the interaction between data and humans or computers. The study concluded that the complete learning kit interacts with the cloud platform as proof of this innovative training solution. Check the following steps to mitigate the upcoming challenges. This is a powerful training solution for educational students who are interested in new advancements in IoT and Blockchain technologies because it not only enhances their knowledge about these technologies but also allows them to have a practical training session via the Cloud platform, which is considered a fundamental factor for any students and new graduates to develop their engineering skills in these emerging fields (Kamal, et al., 2018).

Shahbazi and Byun used Hyperledger Fabric's private Blockchain to structure variable data and test the fault diagnosis prediction and used data mining algorithms that simulated the real-life challenges to complete cascaded testing with Blockchain-based cryptocurrency solutions; the classification output was then used to verify the accuracy of the data. XGBoost machine learning algorithms were also used to read data and offer precise quality evaluation. The ground-breaking point of their system is to use Blockchain in a machine learning algorithm that assists and optimises innovative processing methods and improves environmental quality, providing safer solutions for workspace users worldwide (Shahbazi & Byun, 2021). In the study, Shahbazi and Byun used Hyperledger Fabric's private

Blockchain as an archive for storing all the required data in instream and taking appropriate measures when the fault diagnosis prediction was at risk. Quality control was provided through a data mining solution that offered complex simulations for real-world cases against cascaded testing using a Blockchain-based cryptocurrency solution. The classification output provided a means to validate the obtained data, while XGBoost machine learning algorithms helped obtain the data and provided an optimised score on its quality. The most significant feature of their system is integrating Blockchain technology with machine learning and intelligent processing methods to improve environmental quality (Shahbazi & Byun, 2021). On the other hand, the adverse consequences of the limitations in transaction throughput led to Blockchains not being cost-effective for processing high volumes of data. IPFS is used to process a large amount of data, thus complementing Blockchain as a supporting technology. The scheme has been implemented and proved practically workable through experiments. Zheng et al. have designed an IoT data storage and transmission scheme based on advanced Blockchain and IPFS technologies. The scheme comprises a DAG-based IOTA Tangle, which provides high scalability, low cost, and data integrity in data exchange. IPFS addresses the challenges introduced by large volumes of centralised data. The scheme's implementation and experimental results prove it. Such frameworks can share IIoT data among FoF production systems and play an essential role in formulating data-driven manufacturing strategies (Zheng, et al., 2020).

2.6.3 Enhancing Scalability, Throughput, and Latency in BCoT

Deploying Blockchain in IoT will facilitate a series of operational transformations across several domains by securing interactions, connectivity, and performance across digital ecosystems (Rahma, et al., 2021) (Alam, 2023). Several architectures and frameworks have been proposed to ensure the secure storage of data and its management in the IoT domain by using Blockchain technology to provide security, trust, and efficiency in IoT networks (Košťál, et al., 2019) (Hegde & Maddikunta, 2023) (Baig, et al., 2022). Moreover, applying such a BCoT infrastructure for environmental monitoring and energy management – an area where it has been trialled with notable success – shows the potential to improve sustainable practice and reduce energy usage and reveals the opportunities for this technology to revolutionise society (Sadawi, et al., 2021). Nevertheless, this approach introduces several technological limitations and obstacles, such as scalability, high energy consumption of the Blockchain algorithms, and a lack of adequate and efficient consensus mechanisms. Another category of potential challenges facing BCoT concerns security flaws and vulnerabilities, the complexities associated with distributed connectivity, and the inherent performance limitations of centralised system architectures (Ma, et al., 2023) (Alam, 2020). These constraints emphasise the significance of ongoing research and development in this subject to address practical implementation and scaling problems (Nuss, et al., 2018).

The IoT is primarily structured based on a central server model where all devices must connect to one central server to authenticate, register, or communicate with one another (Domínguez-Bolaño, et al., 2022). Unfortunately, the centralised model poses several drawbacks; most notably, scalability is a cause for concern, and eventually, we will have to proceed to a decentralised model. Conversely, an emerging solution holds the potential to decentralise IoT systems and overcome some of the inherent bottlenecks of the centralised model. Consequently, the fundamental features of Blockchain technology are decentralisation and distributed consensus-based architecture, which makes it the ideal candidate for ushering in decentralisation in IoT. Being secure and tamper-resistant due to the distributed consensus-based nature of its architecture, the Blockchain system, under its governing protocols, boasts a trustless system for all parties on a public network wherein every single action is recorded as an append-only entry, forming the chain. In addition, data redundancy, availability and ease of management are some of the other revolutionary features that make it suitable for the IoT (Habib, et al., 2022) (Al-Nbhany, et al., 2024) (Alkhateeb, et al., 2022).

Several studies discuss the scalability of Blockchain-IoT integration. IoT systems include the use of a private Ethereum Blockchain within the network. There is increased academic interest in integrating this Blockchain into IoT systems, and several studies detail the advantages and disadvantages of this integration, the implications for the use of data in IoT systems, and how security and privacy issues are addressed in this integration. The impact of Blockchain on the scalability of IoT devices was reported by Hang et al., who proposed an integrated Blockchain IoT ecosystem featuring three RPi4 nodes. Three RPis were used to demonstrate how Private Ethereum Blockchain could be used for data management

(Hang & Kim., 2019). Furthermore, a research study shared how Blockchain can further reinforce IoT systems, particularly in decentralised trust management, security, and scalability. A systematic literature review by researchers Hongyan et al. analysed selected Blockchain solutions to address IoT system issues and found how combining Blockchain and IoT can solve current problems (Cui, et al., 2019). Furthermore, another study systematically explores many types of Blockchain technology and their applications in the IoT system, pointing out that decentralised Blockchain governance and trustworthiness management benefit a Blockchain IoT environment. Another survey on Blockchain and IoT convergence by Reyna et al. analysed the chance and the issues of research into Blockchain and IoT engineering (Reyna, et al., 2019).

A survey underlined the applications of Blockchain in integrating IoT systems for improved interoperability, privacy, and security to combat the heterogeneity issues of IoT systems and limited bandwidth and memory issues of IoT devices. A study examined the performance and scalability of the private Ethereum Blockchain. It demonstrated the potential of the Blockchain to enhance the performance, reliability, and scalability of IoT systems (Schäffer, et al., 2019). Another study conducted by Casino et al. also pointed out the challenges in settling payments and interactions in a massive IoT ecosystem of IoT devices and the need for a scalable Blockchain-based system to manage trust. A systematic literature review of the use of Blockchain technology for IoT, outlining the extent to which Blockchain can enhance cybersecurity in IoT systems (Casino, et al., 2019). The study outlined the need for decentralised trust, security, and scalability in a Blockchain IoT environment. Most recently, MQTT throughput improved mainly by HiveMQ, which is worthy of note. HiveMQ, offering MQTT as a service, has improved intra-cluster messaging and higher MQTT throughput, thus improving overall MQTT performance, which is very important, particularly for its integration with IoT and Blockchain. The increased throughput and overall MQTT performance are crucial for IoT (Podolskiy, 2024).

2.7 Evolution and Implementation of Remote Lab Systems

2.7.1 Evolution from Lab 1.0 to Lab 4.0

The first Industrial Revolution profoundly changed society and people's lives by impacting manufacturing, production, and transportation. The development of the first industrial revolution affected the education sector irrevocably, mainly because many modern university and school buildings were built in a factory model. In particular, the first industrial revolution led to the introduction of engineering education in universities because of the shortage of labourers such as builders and craftsmen, who became known as engineers. Then, the classical apprenticeship system of one-to-one exchange of production technology in a workshop was replaced by a product-teaching model from universities and polytechnics, E´coles, and the new applied science type of institutions. Learners acquired practical skills not by reproducing a model within a single workstation, like how the ancient Greek scholars approached experimentation, but by using a new experimental paradigm that turns the advancement of scientific knowledge into a core and central content of engineering education (Lantada, 2020).

The first 'business case' for an experiment date from 430 BC, made by the Greek philosopher Empedocles, who used the clepsydra (a device for transferring liquids from one vessel into another) to demonstrate the corporeity of air. Moreover, in 1595, the Danish astronomer Tycho Brahe (1546-1601) opened his first laboratory at Uraniborg Research Centre (Wolfschmid., 2002). However, the earliest university that created a laboratory for teaching and experimentation purposes was the University of Giessen in Germany, under the guidance of experimental researcher Justus Liebig (1803 –1873), who had practised a chemical-experimental approach to the natural sciences in the 1820s. Liebig's education 1.0 experiment generated a template that other universities started to reproduce, although the model may be described, with a particular abstraction, as lab 1.0. The first version of this research paradigm affected the German-speaking metropolises of education. In principle, any university could be considered as a receptive university to be influenced by this lab-based model. Nevertheless, in the case and early incarnation of laboratory teaching and experimentation with animals, a complex process of transport, transfer, adaption, and translation of the laboratory model took place in universities all over Europe. However, this creation of laboratory infrastructure and practice had less uniform one-dimensional character than a complex process at different linguistic, tool and experimentation technique levels (Chang & Rocke., 2021).

The period from the mid-19th century up to the end of the Second World War was the Second Industrial Revolution, where a rapid succession of discoveries and innovations made it possible and practical to produce electricity steel, harness the power of mass manufacturing, and every other kind of invention, devices, tools, and equipment, and the new materials that they used. A whole industry became established to supply the increasingly crucial area of scientific enquiry, pure and applied, with the laboratory equipment and supplies needed to conduct the research. Now, the programming languages, technologies, production methods, standards and specifications unite the idea of using and working with software in everybody's minds. This tremendous expansion of science and technology dramatically changed the learning practice and revolutionised university and college teaching and research methodologies. It has been dubbed by many scholars ‘Laboratory 2.0’ because it closely follows ‘Education 2.0’, an analogous transformation in the education system. It can be said that Laboratory 2.0 arrived at the universities when the programmes had become well entrenched by the honour of accreditation, faculty-built curricula, and fields of study organised by what might be called occupational and technical demands, both within the university and outside.

Indeed, research and scholarship in science and technology had formal rules and professional systems, structures and conventions that facilitated coordinated and collaborative work. Science groups – not just individuals – would now be essential in creating knowledge production, education and learning at Laboratory 2.0. In many ways, as the house for scientific inquiry changed things, so, too, did pedagogy move in new directions: It was no longer about what the scientist-teacher knew, but how he or she knew, how the knowledge was produced and created (Schmidgen., 2021).

The third industrial revolution, with its origin in the invention of the transistor and its culmination in the generalised use of the Internet to become the ordinary medium of interpersonal and machine communication at the end of the 20th century, contributed to the rise of Lab 3.0. During the era of Education 3.0, when universities became more internationalised, as enabled by the proliferation of accreditation organisations, new programmes, and topics in the field of engineering and science also emerged. A third major shift in education has taken place, with online learning and remote labs as the dominant communication and information technologies that enable the flow of educational processes (Correia, et al., 2021). Remote laboratories have become increasingly popular for delivering education online due to the potential to provide students access to experimental facilities from anywhere on the Internet. Students can perform experiments and engage with experimental parts of their course at any time, breaking the confines of the physical availability of a real laboratory. Additionally, distributed labs allow for greater resource sharing and allow a single device to be shared among multiple institutions. This allows for the collaborative use of mostly expensive, robust equipment and state-of-the-art technologies, mitigating the addition of redundant infrastructure needed in each academic institution. This approach also helps to reduce excess costs because schools do not have to replicate an entire set of hands-on practices. Creating and maintaining a physical laboratory space are not simple tasks and require careful planning, as can be done in a controlled remote lab in another institution (Machotka, et al., 2011). The first remote laboratory transplanted over the Internet was developed at the University of Southern California around a system for remotely controlling an industrial robot via the web (Ken Goldberg, 1995). Over the past two decades, countless remote laboratories have spun up that concern almost every domain of science and engineering in all parts of the world. They are often built and managed according to various architectures, programming languages, technologies, approaches, and learning management systems (Chacon, et al., 2015) (Alkhaldi, et al., 2016).

As the forthcoming industrial revolution ushers in what has been termed Industry 4.0 and Education 4.0, human-to-human interaction finds another level of experience with socialisation beyond physical presence through Laboratory 4.0 to converge people, society, man and machine through the synchronised integration of the natural and virtual worlds (Garcia-Loro, et al., 2021). Following the fourth industrial revolution, we have the paradigms of Industry 4.0, Education 4.0, and Laboratory 4.0. Human and technological components are seamlessly integrated into an ecosystem where an unprecedented productivity space is brought forth through the crossover of the real and virtual worlds.

Industry 4.0 is the term we use to amalgamate state-of-the-art manufacturing with digital technologies to create intelligent, self-optimising production systems. Using CPS will allow data sharing between machines in real time and enable them to make their own decisions, increasing the flexibility, efficiency, and customisation of industrial processes. At the same time as this industry transformation, Education 4.0 seeks to disrupt the way we teach and learn by integrating traditional methods and the latest technologies in ways that allow for individualised and immersive learning, enabling students to acquire the knowledge and skillsets needed for the future of work. Taken together, they comprise an evolutionary leap towards coalescing artificial and natural intelligence for the benefit of humanity. Furthermore, Industry 4.0 refers to the combination of CPS, the IoTs and cloud computing, paving the way to reinvent manufacturing and engineering. Education 4.0 and Laboratory 4.0 converge with Industry 4.0 to further bridge the virtual and physical worlds in education and research. These transformative paradigms unleash the power to create new products and services, discoveries, and innovation, thereby forging a promising future for humans, industry, and learning.

Laboratory 4.0 is realised by applying new technologies, such as AI, Autonomous Robots, Immersive Virtual Reality, Augmented Reality, Data Analytics, Internet of Things, 3D Animation, Remote Collaboration, Network Information Computing, 5G Communication Networks and massive wireless sensors to deliver the university's highest quality in real-world practical training, educational competency, assembly industry, and real-time tutorial. Potentially, it will be the most transformative educational support system that is harnessed to drive the engineering academic advancements and equity in education for all humanity if technologically developed and adequately integrated with content to be utilised in each backchannel of the teaching process in the classroom, and lifelong learning beyond the university campus (Garcia-Loro, et al., 2021).

2.8 Chapter Summary

Chapter 2 provides a comprehensive literature review on the intersection of Blockchain technology and the Internet of Things (IoT), focusing on the Blockchain of Things (BCoT). It begins by introducing Distributed Ledger Technology (DLT), explaining its foundational principles and how it underpins Blockchain. The chapter categorises various types of Blockchain networks, contrasting permissioned and permissionless systems, and discusses different consensus mechanisms that ensure transaction validation.

The review further explores specific Blockchain platforms and off-chain solutions like IPFS, emphasising their roles in enhancing data management. It also delves into integrating Blockchain with emerging technologies, including artificial intelligence and cyber-physical systems, highlighting the potential benefits for IoT applications. Additionally, the chapter addresses the synergy between IoT, big data, and Blockchain, discussing how these technologies collectively enhance scalability, throughput, and latency in BCoT systems. In addition, the chapter examines the evolution of remote lab systems in education, illustrating how Blockchain can secure and manage data effectively within educational frameworks. This literature review sets the stage for the subsequent chapters by identifying gaps in current research and establishing a foundation for the proposed BCoT architecture.

The next chapter, 3, Research Methodology, deals with the research philosophy, basic methodological principles, and methodology on which the study is based. It outlines the experimental method, the schedule, and the techniques and procedures used for data analysis. Chapter 3 includes an elaborate roadmap of the strategies employed to ensure the robustness and soundness of the study.

Chapter 3

Research Methodology

3.1 Introduction

The research methodology outlines the systematic approach employed to investigate the performance of BCoT systems, focusing on scalability and efficiency enhancements. The initial phase involves establishing a robust research philosophy, which guides the selection of appropriate strategies and techniques. A mixed-methods approach is adopted, integrating qualitative and quantitative methodologies to ensure comprehensive data collection and analysis. Experimental methods are emphasised, particularly in performance testing, where metrics such as latency, throughput, and resource utilisation are meticulously evaluated. This chapter also details the research choices, including the time horizon and specific data gathering and analysis techniques. Furthermore, the methodology incorporates a detailed description of the experimental setup used to validate the proposed BCoT architecture. Key components include deploying a private Ethereum platform integrated with IoT sensors and edge computing solutions. Performance evaluations use tools like Geth Metrics to assess improvements over existing frameworks. The findings reveal significant advancements in system performance, with reductions in latency and throughput increases, demonstrating the proposed architecture's effectiveness in real-world applications. The methodological rigor established throughout this investigation reinforces the validity of the results and contributes valuable insights into future research directions within BCoT systems.

3.2 Research Philosophy

There are many research methods and models, each with advantages and disadvantages. "The Research Onion" is one of the most famous and complete research frames. Research onion and nested methods are commonly used research frames (Saunders, et al., 2003). Figure (10) shows the research onion frame:

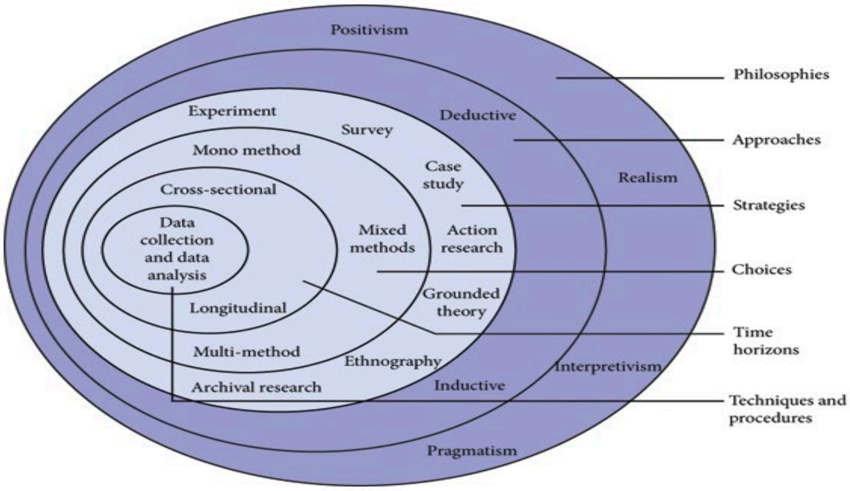


Figure (5): Saunders research onion model.

Each layer addresses one specific aspect of the research and depicts the variation in the paradigms, strategies, and choices that the research phenomenologist uses throughout the research project. It shows the significant questions the researcher must consider in any research project. The model consists of six layers: the epistemological position of the researcher, the approach, the research strategies and choices, the temporal dimension of the project and the data collection tools used by the researcher (Mishra, et al., 2015). This general framework is inherently interdisciplinary and hence can be adapted to several disciplines, which is undoubtedly a positive for its research use. The framework has been applied to prior work on BCoT systems.

In light of the scientific research philosophy for the development of an Interoperable BCoT for scalable and efficient IoT Data Management on top of Ethereum Blockchain, a pragmatic approach based on a mixed-paradigm (positivist and interpretivist) philosophy is considered suitable given the study aimed at being both exploratory and confirmatory, where foundational ideas and theoretical constructs can be validated empirically by relying on sensor measurements and Blockchain transaction data (positivism). At the same time, designing and implementing a new Blockchain-based storage model involves understanding the context and implications of the technology applicable in the real world (interpretivism).

The philosophical foundation of this work is rooted in the reality that the world is not only complex but also dynamic and needs a complementary research practice that bends to the needs of the study. This is particularly important when exploring the interfacing of networks of Blockchain and IoT devices. Knowledge here is not a timeless medium; it is a construct borne of the ongoing emergence of phenomena observed and the embodied and situated experiences and interpretations attributed to the human actors exploring and building BCoT. The philosophical stance embraces the complexity of the entangled behaviours and phenomena between the Blockchain and the IoT devices and the need for a methodology that can respond to changing technological conditions. This dynamic and flexible perspective should enable the study to capture nuances and intricacies due to the fusion of both technologies and contribute to a more extensive understanding of the challenges and opportunities of deploying this technology (Mishra, et al., 2015).

This philosophy is also underlying the research goals that include the design of BCoT based on case-based reasoning that will communicate to each other and with a user using web services and data files; the provision of a Blockchain data storage model for BCoT resting points along with environmental and healthcare parameters collectively generated by BCoT modules and sensors; and experimental assessment and measuring (offline and online evaluation) to validate the overall expected and proposed scalability and performance for BCoT.

This research philosophy is reinforced by the chapter of the descriptive literature review (Chapter 2), which explains why the adoption of a Blockchain technology paradigm has a solid potential for reforming IoT systems by providing a transparent system with the confidence that information and assets cannot be tampered with; by automatically resolving the data redundancy, inconsistency, availability and ease of system management issues; and by creating a decentralised architecture providing safe exchange of data from all network nodes.

This study's pragmatic and multidisciplinary research philosophy involves examining data empirically and identifying a context- and technology-driven framework in which an interoperable BCoT data management using an Ethereum-based Blockchain has been effectively conceived and implemented.

3.2.1 Research Approach

The deductive research approach is employed in this study to implement the Blockchain theoretical research framework for testing the hypotheses, which primarily address the issues of evaluating the scalability and efficiency of data management in IoT applications leveraging BCoT environment context awareness. It is an inductive quantitative research approach grounded in deductive logic to provide positive or negative evidence for the predefined hypotheses derived from the theoretical frameworks (Gabriel, 2013).

Theoretical Framework and Hypothesis Formulation: The thesis begins with a thorough literature review, elaborating on BCoT's theoretical basis and its potential to overcome the limitations of client-server models. This provides the ground for specifying hypotheses, such as that a Blockchain-based storage model will equip BCoT devices with much higher and more robust data integrity and confidentiality than any conventional storage model.

Empirical Testing: After the hypothesis is established empirically using the scientific method, the research uses a structured experimental configuration to test the hypothesis empirically at various levels, including qualitative process and quantitative. For instance, this research will test the hypothesis across two levels: a new Blockchain-based storage prototype that will be deployed in a private network of the research team using RPi4 nodes and different IoT devices to simulate a real-world BCoT environment, and the post-deployment, the performance of the proposed architecture model will be evaluated against performance metrics (such as System Latency, Transaction Throughput, Scalability, Resource Utilisation…etc., which is used to assess the hypothesis for or against statistically.

Comparative Analysis between IPFS and FTP: To contextualise the scale of the IPFS results, this research uses FTP as the reference for comparing the performance of the off-chain storage solution. The proposed Blockchain-IPFS-based architecture is compared to FTP storage implementation to reflect the relative advantages of the proposed approach and point out the scalability and efficiency of its implementation of IoT data management in a BCoT.

Methodological Rigor: The deductive approach has methodological rigour. For example, research questions generate hypotheses, focus the research, and tend to be unambiguous. The obtained empirical evidence is reviewed accordingly, with hypotheses either rejected or confirmed based on the empirical testing. It is a rigorous way of approaching research questions and moving the understanding forward regarding Blockchain as an essential architecture for enhancing the scalability and efficiency of IoT systems.

Contribution to Knowledge: This study's empirical evidence contributes to the field of knowledge by highlighting the capabilities and challenges of Blockchain technology in addressing the challenges of the IoT. Based on the deductive research approach, the study's findings have provided important insights for designing and implementing BCoT with innovative, scalable, and efficient IoT solutions.

This study attempts to offer valuable contributions to the field by adopting the deductive research approach, which aids in investigating the hypotheses through its systematic process of bringing empirical data and comparative analysis. The empirical evidence presented in the study brings valuable insights into the discourse on Blockchain technology's potential role in revolutionising IoT data management to ensure efficient operations and high security in the era of IoT and Industry 4.0.

3.2.2 Research Strategies with Experimental Methods

The thesis employs an empirical approach to examine these issues with an exploratory case-based study and experiment-based validation to help improve the robustness and efficiency of Blockchain solutions to address the scalability and performance issues in IoT and implement solutions in a real-world private Ethereum Blockchain, leveraging unique techniques and methodologies.

Experimental Validation: It is important to note that experimental validation plays a crucial role in the evaluation of the proposed Blockchain integration in IoT applications. In this chapter, we investigate two real-world use cases of IoT and Blockchain technology, including a remote laboratory management system and a machine learning-based real-time triaging of ICU patient vital signs. The remote laboratories form a distributed testbed to build an interoperable CPS consisting of a dedicated hardware, networking, and management platform, which facilitates the study of the overall system performance.

Each of these CPS agents are attached to an RPi4 node, each containing a chain of sensors that are communicating, mining, and propagating new blocks, which is the core engine of the experiment. In the Ethereum case, the IoT devices are physically embedded in the system. The key performance metrics – system latency, throughput, and energy consumption of the IoT devices – were measured as part of the application’s performance benchmarking. It is a robust performance evaluation process that allows us to evaluate whether and how fast Blockchain integration fits in an IoT environment and whether the system can meet the performance requirements.

Innovative Techniques: Advanced approaches, such as edge-computing on the RPi4 nodes, allow the processing and storing of IoT data locally before being channelled to the Blockchain. Finally, integrating MQTT, AI, an IoT communication protocol optimised for integration with the Blockchain, increases the communication efficiency between IoT devices and the Blockchain. Identity management, authentication and access control mechanisms further reinforce security and privacy for IoT-device interactions with the Blockchain.

Smart Contract Implementation: The study uses smart contracts on an Ethereum PoA implementation to control specific nodes in IoT systems, such as sensor data storage and actuator control. Such smart contracts designed, developed, and optimised to interact with IoT devices. The PoA consensus protocol would be a scalable solution for integrating IoT systems to enhance operational efficiency.

Data Visualization and Analysis: Organising a data flow and then visualising it helps the coding process. Node-RED is a visual programming tool used to model the data flow in a process. Integrations with InfluxDB and Grafana contribute to data visualisation and aid in making sense of the information gathered about the system's operation. Further, a small amount of IPFS is used for off-chain storage as a means of additional data storage capability.

Novel Architecture Proposal: The key highlight of the proposed research strategy is a novel Blockchain architecture connecting resource-bound sensor IoT devices to the private Ethereum Blockchain via RPi4 gateways’ that overcomes the critical security, connectivity, scalability, performance, and efficiency challenges in IoT to Blockchain integration scenarios. It also assists with handling the volume, velocity, and variety of IoT data. By combining case-based exploration with experiments validation methodologies and innovative integration methodologies for Blockchain in IoT application developments, the proposal anticipates exploiting the potential of private Ethereum open Blockchains through scalability constraints and efficiency enhancement of Blockchain solutions. The systematic steps in the experimental deployment highlight the rigour in validating the proposed case-based solutions to the stated research objectives.

3.2.3 Research Choices

The study choices are based on a quantitative research approach employing numerical data analysis methods specific to three performance indicators: transaction throughput (TPS), system latency, and resource utilisation. The research method alignment serves the purpose of the study as a rigorous quantitative analysis that evaluates the proposed Blockchain-based solution addressing various data loads and conditions. The mono-method quantitative research design allows systematic exploration and a non-biased view of three key performance metrics: scalability, latency, and throughput at varying data loads. The approach enhances the reliability of the study findings as numerical data are explored and used as evidence for the proposed Blockchain system's efficiency and effectiveness.

Besides, using quantitative research methods will make it possible to disclose the system's performance metrics in detail and consequently assess the reliability and efficiency of the BCoT proposed architecture. Quantitative research methods will allow drawing empirical conclusions about the relevance of integrating AI, IPFS and MQTT into the system and the consistency of the real-time scheduling system and priority classification methods with its ideal type. Adapting the methodological framework from a mono-method, quantitative research reduces the chance for theoretical generalisations and predetermined conclusions in a study. However, it allows for a direct and transparent data analysis aiming for relevant and truly empirical results.

In terms of answering the research question, the chosen method supports driving the knowledge forward to reach a deeper understanding of Blockchain integration into IoT systems, especially integrating real-time, priority-based, and decentralised data scheduling into the BCoT proposed architecture. This approach allows for an unbiased and quantitative justification of the research, making the selection of technological solutions more reliable with statistics and empirical results backing the proposals, thus contributing to solving the revealed research gap on the tension between the decentralised and shared approach to

Blockchain storage and the requirements of scalable and efficient BCoT proposed architecture on the IoT.

3.2.4 Time Horizon

Some sliding-scale timelines illustrate the time horizon for deploying and practically using an interoperable CPS, including the fusion of Blockchain with IoT applications. In the short term, in the immediate future, the scheme highlights implementing an architecture composed of three nodes for mining and spreading new blocks located in remote laboratories.

The short-term temporal horizon concerns the initial installation and configuration phase. It includes programming microcontrollers for two-way communication with RPi4 through the MQTT protocol and communication with the Ethereum Blockchain for interaction with smart contracts using the Web3.js library. Node-RED is configured to communicate with the chosen smart contracts, read their data, and process it using JavaScript functions.

The middle-term horizon is set to use edge-computing techniques within each Raspberry Pi 4 node to collect and process IoT data with the Blockchain and enable IoT sensor data to be processed and stored at the edge rather than at the source, which involves immediate scalability and performance optimisation. The scheduling of business activities at that point is set under a period of deploying an Ethereum PoA client and IoT-specific smart contracts at each node.

The very long-term time horizon is continuous refinement and scaling reflected through best practices that incorporate IPFS for network-enabled, additional off-chain storage; enduring evolution and adaptation of the functional, distributed, wireless, and resilient architecture that can scale and adapt over time; and the refinement and testing of the PoA consensus protocol as an efficient way for and with IoT-enabled Blockchain.

Within these time horizons, these challenges are recast as iterations, detailing when and how security, connectivity, and performance problems will be ameliorated through the implementation of identity management, authentication, and access control mechanisms. Identity management, authentication, and access control are thus envisioned as both asynchronous and recursive processes and never as singular and already accomplished processes.

Time Horizon ensures that this project's IoT-Blockchain architecture deployment covers not only the immediate steps in scheduled events and addresses the challenges of present-day IoT-Blockchain issues but also explores the future steps of this technology that will enable the timeline of systematic long-term exploration and improvement for IoT-Blockchain integration.

3.2.5 Techniques and Procedures

The integration of the Interoperable CPS for scalable and efficient IoT Data Management with the Ethereum Blockchain to perform transactions of tagged data originating from the IoT devices, the allocation of computational resources to execute smart contracts among the different users of the system, followed a structured procedure for evaluating the effectiveness of IoT applications enhanced by Blockchain and for performing exhaustive performance analyses. This architecture was deployed and tested with direct application to remote laboratories and machine learning-based real-time triaging of intensive care unit (ICU) patient vital signs through, on one side, the rigorous use of new techniques and methodologies for overcoming scalability, performance and security issues that have been observed in current solutions.

System Components: The architecture contains three RPi4 nodes (B 8 GB) that mine and spread new blocks. Figure (11) illustrates the physical architecture components. The architecture can have more nodes, and each node has distinct roles. The significant roles are mining and spreading new blocks.

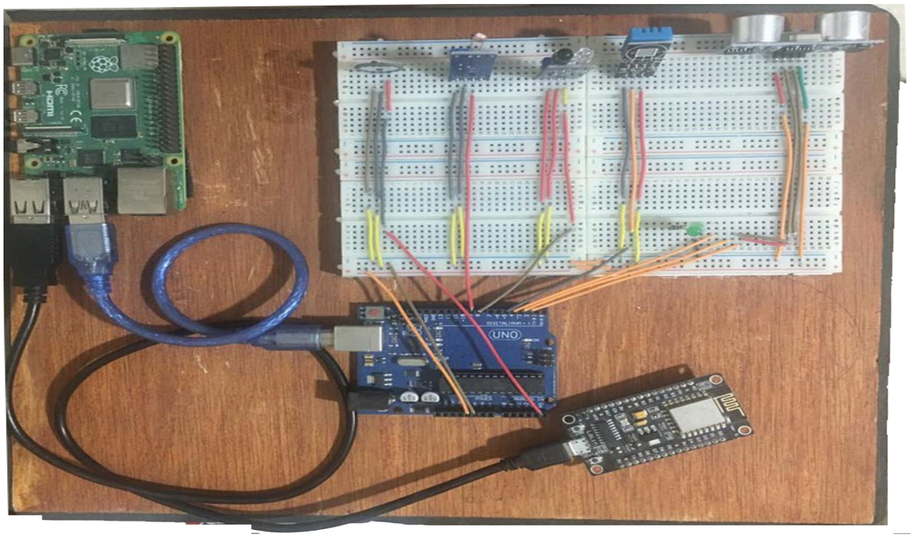


Figure (6): Snapshot of an example of a microcontroller implemented in the system.

Innovative Approaches: The latest approaches to these technologies were utilised to overcome the other implementations' scalability, performance, and security shortcomings. The implementation of edge-computing techniques on the RPi4 nodes allowed for the processing and storage of IoT data locally before it was merged with the Blockchain. MQTT was a specialised communication protocol for IoT and Blockchain integration, enabling data mobility between devices and the Blockchain.

Identity Management and Access Control: The Ethereum Blockchain was leveraged in this use case to improve identity management, authentication, and access control of IoT devices interacting with the network, ultimately increasing security and privacy. Each node ran an Ethereum PoA client. The smart contract logic allowed for efficient execution and data storage on the Blockchain. For this use case, new smart contracts were developed for the various parts of the IoT application: sensor data storage for different applications, actuator control. For each part, performance considerations were considered.

Private and public keys were a key part of the network's security architecture. Each IoT device was assigned a unique pair of cryptographic keys: one private key for signing transactions and another public key, both to identify the device in the network and allow others to verify the device's public key. This allowed the device to communicate with others in the network securely. A Metamask wallet – an open-source browser extension that acts as a cryptocurrency wallet, providing an easy-to-use interface to interact with the Blockchain – was used to manage the keys on the device. This setup meant only a device with the proper cryptographic key could participate in the network. This prevented any interference or malicious activity from unauthorised parties.

Data Visualization and Analysis: A powerful tool, Node-RED, was used as a front end to visualise the data flow through the system. This required integrating dashboards and modules to control the system. In addition, InfluxDB and Grafana, professional-grade tools, were added to the mix for data visualisation and analysis. In contrast, IPFS was added as an off-chain storage component, further enhancing the system's capabilities.

Novel Architecture: A notable achievement of this field deployment was the novel AI-enabled architecture, further expanded when supervised and unsupervised AI algorithms were integrated into RPi4 gateways to connect the bare minimum IoT devices with the Ethereum Blockchain. Such an AI-powered architecture could ensure the respective security, connectivity, and performance requirements for a distributed Blockchain platform to process the ‘3 Vs’ of data in an IoT architecture complied with the Blockchain paradigm: volume, velocity, and variety.

Deployment Steps: All the microcontrollers were programmed using Arduino IDE and Python for MQTT communication with the RPi4 nodes. Node-RED was configured to work with the Ethereum Blockchain via the Web3.js library. It allowed data to pass between smart contracts and IoT devices as sensors capture data; it was stored on the Blockchain and IPFS through Node-RED functionalities. This way, data are effectively distributed across a peer-to-peer network to prevent redundancy.

Data Analysis: The next phase of the study is data analysis, where multiple metrics used and tools to examine the Geth metrics, along with InfluxDB, MQTT, and Node-RED, for visualising, analysing, and storing data.

Geth Metrics: Geth metrics allow the tracking of the performance and behaviour of Ethereum nodes on the private Blockchain. They can monitor timestamps on blocks and transactions, the time it takes to mine blocks, remote node uptime, connection status, node-to-node polling intervals, etc. These can be used to glimpse overall network health, transaction time and time-to-live of blocks and transactions, and node performance and bandwidth usage.

InfluxDB: For data processing, the InfluxDB database is used to load historical data from the validator nodes. This robust time-series database can store and handle large blocks of time-stamped data, such as those produced by IoT devices and Blockchain transactions. In this way, InfluxDB stores the historical data of the performance results, system metrics, and transactions processed for further analysis and visualisation. This database can easily retrieve information and display the concrete data points required for performance analysis and optimisation.

MQTT: The MQTT protocol ensures efficient communication between all IoT devices and Blockchains. As a lightweight protocol messaging, MQTT ensures the efficient capability of dataflow between all devices, transferring data efficiently from one device to another or sensors to the broker and then uploading to the Blockchain. The speed and reliability of the totals system depend highly upon the MQTT protocol, which enhances the capability of all devices in the network to communicate.

Node-RED: Node-RED is a robust visual programming environment that orchestrates data flow between IoT devices, Ethereum Blockchain nodes, and any external database into which sensor data needs to be stored (Using InfluxDB). Node-RED provides a simple and intuitive scripting environment and leverages the Web3.js library, developed by Ethereum for handling Ethereum-related interactions, to invoke smart contracts, retrieve data from processed Blockchain transactions and deal with sensor data efficiently (i.e., without unnecessary redundancy). Thus, Node-RED can provide the necessary glue to stitch together a working system capable of adequately handling and processing requests that may originate from various IoT devices in various countries. Node-RED can also be leveraged to drive data transformations and enrichments before it is appropriately visualised using InfluxDB and MQTT. The seamless integration between Geth metrics, InfluxDB, MQTT and Node-RED thus provides the solid foundations for conducting performance analyses that allow us to derive valuable insights from the IoT-Blockchain ecosystem. In total, this framework proved versatile and powerful enough to enable us to continuously monitor system performance, perform the necessary analysis on transactions executed on the system, visualise the critical data corresponding to the measures used in our algorithm, and ultimately ensure proper interactions between the IoT devices and the Ethereum Blockchain.

3.3 Chapter Summary

The research methodology employed in this study is structured around a comprehensive framework that integrates various philosophical approaches, strategies, and techniques. The investigation is grounded in a pragmatic philosophy, which allows for applying both qualitative and quantitative methods. The approach is primarily experimental, focusing on developing and testing a novel BCoT architecture. Data collection involved a mix of primary and secondary sources, with experimental methods being utilised to assess the performance metrics of the proposed architecture. This included latency characterisation and resource utilisation analysis using tools such as Geth Metrics. The research design also incorporates a longitudinal time horizon to ensure robust data collection over an extended period, facilitating a thorough evaluation of the system's scalability and efficiency.

The methodology outlines specific procedures for implementing the BCoT architecture, including integrating IoT sensors, edge computing, and IPFS for decentralised data management. Techniques such as Random Forest classifiers were employed to process sensor data in real time, achieving high accuracy rates in predictive analytics. Performance evaluations demonstrated significant latency, throughput, and resource utilisation improvements compared to existing solutions. The methodological rigor ensures that findings are reliable and can be generalised across similar contexts within the field.

The next Chapter 4: Design of a Proposed Novel BCoT Architecture, this chapter describes the design, initialisation, testing and deployment of the proposed IoT-Blockchain platform. The integration of Ethereum Blockchain and PoA with Raspberry Pi nodes, edge processing, data collection and storage will be described. The efficiency and security of Ethereum’s Clique PoA protocol in the BCoT ecosystem will be analysed. A detailed version of the proposed architecture for a BCoT-based Lab system.

Chapter 4

Design and Proposal of a Novel BCoT Architecture

4.1 Introduction

Integrating IoT devices with a Blockchain framework like Ethereum in a resource-efficient manner can significantly enhance the security and performance of decentralised systems. Low-power IoT devices, designed for prolonged battery life, play a crucial role in any decentralised architecture utilising the Ethereum Blockchain. These devices can maintain decentralised communication while benefiting from the robust security features inherent in the Ethereum network. Central to this architecture is a microcomputer, specifically a Raspberry Pi 4 equipped with 8GB of RAM, which is a critical gateway. This microcomputer facilitates communication between the IoT network and the Ethereum Blockchain, acting as an intermediary and translator. The interaction between these technologies occurs through two primary methods, forming an essential part of the Blockchain of Things (BCoT) ecosystem, as illustrated in Figure 12.

This chapter emphasises that the primary direction of interaction is unidirectional: IoT devices utilise Blockchain functionalities rather than vice versa. It explores the interconnected challenges faced by both Blockchain and IoT, including issues related to security, communication protocols, and the resource-intensive nature of maintaining Blockchain systems. Furthermore, it introduces an innovative architecture and advances the design of smart contracts, proposing a Proof of Authority (PoA) consensus protocol to achieve consensus. The chapter also discusses edge computing architectures, data governance, and decentralised applications tailored for IoT environments.

A significant observation regarding current enterprise-level Blockchain applications for IoT is that many remain in the design stages. Future research should focus on developing practical Blockchain and IoT applications for generalised scenarios where security and privacy are paramount. Additionally, it is essential to explore how to implement Blockchain technology on resource-constrained devices, which could enable real-world applications across various sectors such as healthcare delivery, intelligent energy systems, finance, logistics, and industrial operations. While the integration of Blockchain and IoT technologies is still nascent, ongoing technical advancements promise to create more secure and transparent communication within IoT networks. This progress paves the way for the near-term development of practical applications ready for production use, potentially leading to transformative impacts on a macroeconomic scale across multiple industries.

4.1.1 BCoT Architecture Design

To evaluate the impact of Blockchain integration in IoT applications and perform overall performance reviews/measurements on transaction throughput and system latency, an interoperable BCoT-CPS was implemented and evaluated, featuring a distributed Blockchain ledger, particularly in remote laboratories. A proposed architecture consisted of three RPi4 (model B 8 GB) devices. Each node is assigned to mining and disseminating new blocks. Figure (12) shows the main components of the architecture.

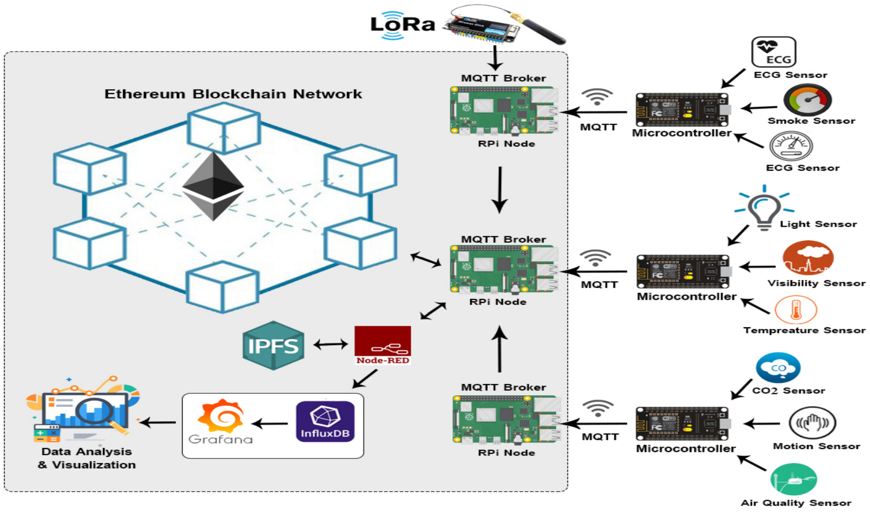


Figure (7): Pilot BCoT architecture design.

RPi4 nodes represented the authorised signers (miners). The system used the private Blockchain platform Ethereum and employed PoA and smart contracts. It consisted of three physical nodes. Each unit was composed of multiple microcontrollers, such as Arduino UNO, Arduino Nano ESP32, ESP8266, and Raspberry Pi Pico W, connected to a set of various sensors, which in our case included mainly a LoRa receiver. Arduino microcontrollers were serially connected to Raspberry Pi 4 nodes, while other types connected via Wi-Fi.

These microcontrollers can be fitted with various sensors to feed the Blockchain nodes with data. For example, biometric sensors measure heart rate and temperature and provide data for healthcare, fitness, and building occupancy detection. Ultimately, the choice of sensors depends on the application under investigation and the data being collected. Regardless of the sensor type, MQTT's versatility ensures seamless integration and efficient data flow within the architecture.

4.1.2 BCoT Architecture Initialization, Testing and Deployment

The combined Blockchain and IoT architecture was studied to overcome the challenges of Blockchain scalability, efficiency, and security issues. Specifications for using the edge computing concept on the RPi4 were provided, leveraging the local availability of processing capability (local computing) and the local storage of IoT data. Before sending the processed IoT data into the Blockchain network, the MQTT protocol was proposed as a reliable communications backbone within BCoT's framework.

MQTT was a critical piece of the puzzle for optimising data acquisition and communication in the system. Its lightness makes it well-suited for resource-constrained devices such as a microcontroller on an RPi4 node. The publish/subscribe nature of this protocol further reduces resource consumption, minimising the need to poll the sources of information and consequently decreasing the network traffic to brokers and the workload of the devices. Moreover, the added scalability and redundancy of this protocol made a difference. The MQTT broker acts as the shared central hub, allowing many devices and PoA nodes to concur and promptly and efficiently exchange data. The loose coupling of this data flow enabled the system resiliency: if, by chance, one of the PoA nodes fails, the system is still almost intact.

The real-time feature of MQTT is also vital to applications that require timely acquisition and control. The relatively simple TCP URL suits data delivery, remote management, or actuation. The three QoS options provide choose-at-your-own-risk: QoS 0 means no guarantee for a message being delivered; QoS 1 means the server guarantees the message will be delivered at least once; QoS 2 means the server guarantees only a single copy of the message is delivered even when there are multiple subscribers to a topic. The combination of MQTT and an MQTT broker provides a highly efficient, scalable, and real-time solution to acquiring and controlling resource-constrained entities in the IoT. The interoperable CPS uses a scheme for identity management, authentication, and access control for the IoT device interacting with the Blockchain.

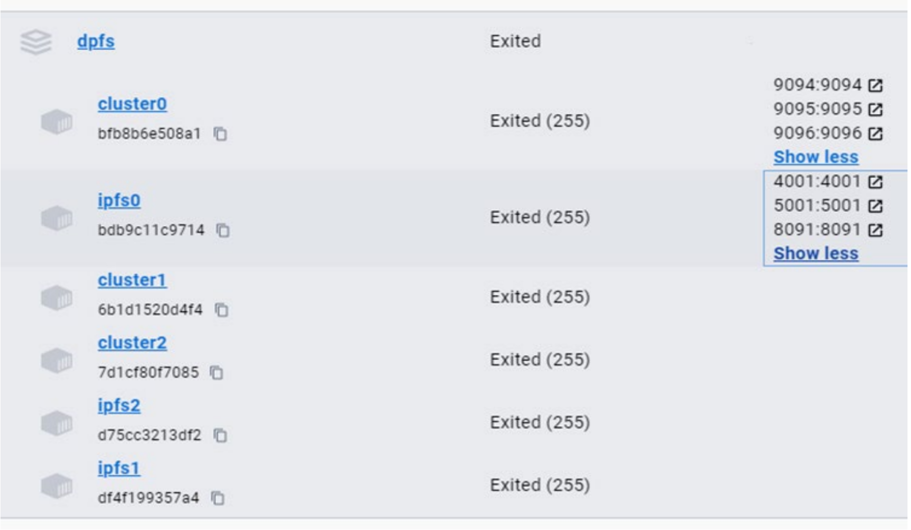
The BCoT architecture has a clear structure that uses the advantages of IPFS, IPFS-Cluster, and Docker to create a highly flexible distributed storage management system. In structure, the architecture takes advantage of decentralised and distributed storage in IPFS with three data nodes as data backup. IPFS Cluster will orchestrate pinned content and replication among the nodes to ensure the desired content availability. Docker containerisation provides more flexibility and portability, so the system can quickly adapt to different requirements. This architecture enables to automatically handle the need for data redundancy, content availability, and data management in decentralised environments with the highest reliability, scalability, and efficiency.

The architecture's data flow is simplified by using a visual programming tool called Node-RED to wire together the hardware devices, APIs, and online services: it has a browser-based editor that makes it easy to wire together flows from a palette of nodes that can be deployed to Node-RED's runtime. Node-RED was connected to the open-source time-series database InfluxDB so it could store and retrieve time-sensitive data created in Node-RED and connect to the open-source analytics and visualisation platform Grafana so users could produce interactive and professional-grade visualisations of their InfluxDB time-series data. Furthermore, Geth metrics were hooked up to Grafana in a stack that provides a comprehensive and powerful toolset for monitoring, analysing, and optimising the performance of a Geth private Ethereum Blockchain. This combination allows operators and end users to ascertain the health, efficiency, and resource utilisation of the Blockchain, helping them to predict and thus prevent performance catastrophes.

Then, an Ethereum PoA client was installed and configured for each node. Finally, a smart contract was programmed, deployed, and optimised on the Blockchain network to enable specific IoT functionalities such as storing sensor data and devices controlling actuators. The PoA consensus protocol was then analysed and suggested as the most efficient and scalable solution for the proposed BCoT architecture. This research effort successfully proved the feasibility, viability, and performance of resource-constrained BCoT architecture to solve IoT's security, connectivity, and performance challenges. It also implemented and demonstrated a solution for the volume, velocity, and variety of IoT data using Blockchain technology.

4.2 Scalable and Redundant IPFS Network Architecture Using Docker Containers

A Docker Desktop IPFS network with six containers typically consists of three containers IPFS nodes and three containers IPFS cluster nodes, as shown in Figure (9).



dpfs	Exited	
cluster0 bfb8b6e508a1	Exited (255)	9094:9094 9095:9095 9096:9096 Show less
ipfs0 bdb9c11c9714	Exited (255)	4001:4001 5001:5001 8091:8091 Show less
cluster1 6b1d1520d4f4	Exited (255)	
cluster2 7d1cf80f7085	Exited (255)	
ipfs2 d75cc3213df2	Exited (255)	
ipfs1 df4f199357a4	Exited (255)	

Figure (8): Docker list of IPFS containers.

This architecture combines IPFS, the Cluster and Docker to create a robust, redundant, distributed content management and delivery network. The triple redundancy of three IPFS nodes deployed in three standalone Docker containers is essential to the network's architecture. These nodes act as content store-and-share hubs for all content on the network so that, even if any single node goes down, replication mechanisms dictate that the data remains available in other nodes throughout the network. Complementing the IPFS nodes were the three IPFS Cluster nodes, also encapsulated within the Docker containers. These Cluster nodes are essential for orchestrating content-pinning strategies across the IPFS nodes. This orchestration boosts data availability and allows for efficient content replication. Consequently, content can be reliably accessed and maintained, even in dynamic and potentially unstable network conditions. The advantage of this Docker container approach was that it allowed for easy network scaling by adding or removing containers to adapt to the evolving data and traffic requirements. Isolation introduced by Docker ensured that each component operated independently, minimising conflicts of operations in the system. Portability with Docker container facilitated uniform deployment across various environments. From developers' laptops to testing and production cycles, deployments can be easily orchestrated with Docker and Docker Compose. Resource-wise, Docker improves hardware utilisation through efficient deployment and management with tools like Kubernetes. As IPFS, IPFS Cluster and Docker are integrated into one system, these containers form a highly resilient and adaptable yet efficient data storage and delivery system. It addresses the range of challenges in data storage, such as redundancies, high availability, and ease of management across a wide range of applications, from decentralised applications and web services to content storage and delivery or even permanent content archival systems.

4.3 Ethereum Blockchain and PoA Integration with RPi4 Edge Nodes

The Ethereum Blockchain network can use the peer-to-peer network to support dApps and smart contracts in its built virtual computer engine called the EVM. This decentralised peer-to-peer system enables wireless access and broadcast of information and transactions from one peer node to all other peer nodes in the system. However, the propagation time of these transactions depends on the robustness and dependability of the underlying wireless network infrastructure. If the wireless network is robust enough, the transaction propagation will be fast, leading to faster, efficient, and timely transaction processing.

Since both these goals promised to be nontrivial, the other half of the computational workload was distributed to proximate edge devices, such as the RPi4. This architecture accomplishes two things that are both crucial: (1) data is processed and stored locally on edge, well in advance when it reaches the Blockchain network, significantly lowering the burden on the limited hardware resources of this network; and (2) many data points can be processed simultaneously, improving efficiency. Additionally, different security measures have been employed to prevent malicious entries by unauthorised parties. For example, we use an official protocol called MQTT to have a potentially universal abstraction layer as a foundation for receiving and forwarding all sensor data to or from the server. This allows us to ensure that all sensor data being received is formatted correctly for the specific task at hand, which increases the system's reliability and efficiency.

In the proposed BCoT architecture, an Ethereum PoA client is installed and configured on each RPi4 node; moreover, the smart contract has been programmed, deployed, and optimally configured on the Blockchain network to enable the desired IoT operations, such as sensor data persistence and actuator control. The PoA consensus protocol is preferred. It is one of the most promising approaches to designing the proposed BCoT architecture and one of the most efficient and scalable in the current IoT landscape.

Through this research endeavour, the feasibility, viability, and overall performance of an IoT-constrained BCoT architecture has been successfully demonstrated to address underlying security, connectivity, and performance issues prevalent in IoT. By capitalising on the respective merits of IoT and Blockchain technologies, this hybrid system implements a data processing solution to explore the simultaneous benefits of handling IoT significant data volume, velocity, and variety by leveraging Blockchain-inspired characteristics to maintain data integrity, transparency, and immutability.

Scaling offers several benefits, notably the lightweight and energy-efficient characteristics of the Proof of Authority (PoA) consensus mechanism, which aligns well with the CPU capabilities of Raspberry Pi 4 (RPi4) nodes. This network can effectively distribute computing tasks, addressing processing, coordination, and storage requirements in a balanced manner. For instance, data processing and storage can occur locally at the edge, alleviating the load on the Blockchain network and thereby enhancing performance. Utilising RPi4 nodes as edge devices facilitates more efficient data filtering and processing before it reaches the broader Blockchain network. Irrelevant computations are eliminated before involving the network, significantly reducing the strain on the Blockchain. In addition, a decentralised edge can perform some computational offloading that would otherwise burden the Blockchain network, thus improving its overall efficiency. Instead of overwhelming the Blockchain network with numerous transactions, it is logical to track only the significant ones. Hence, the PoA consensus protocol eliminates the necessity for computationally intensive processes like mining, which are common in other consensus mechanisms, such as Proof of Work (PoW). This further decreases the system's energy consumption, making it suitable for systems with limited entropy.

4.3.1 Edge processing

Edge computing plays a crucial role in BCoT by helping the system to perform better and more securely. Rather than streaming raw sensor data to the Blockchain, each RPi4 node effectively functions as a powerful mini-processor. Using the MQTT protocol, Raspberry Pi nodes can communicate with each other and resource-constrained IoT devices, streamlining point-to-point communications. These nodes can perform extensive filtering and analytics on the sensor data before sending this data over the Blockchain, effectively reducing network traffic and shaving milliseconds off latency. Each node can operate as a localised processing hub, making real-time informed decisions by applying if-else rules to sensor readings.

This capability negates the need for centralised command-and-control intervention in changing circumstances and allows the BCoT to respond to emergent situations with data fresh from the source. Moreover, given how edge processing keeps sensitive data close to its generative source, these nodes can add extra resilience to the system against cyber-attacks. With edge computing capabilities, the BCoT architecture can withstand certain kinds of disruptions to either the Blockchain or central servers. Overall, edge computing is indispensable in BCoT, optimising performance, securing the system, and enabling real-time control while operating on the system's periphery.

4.4 Data Collection and Storage

The BCoT architecture has been designed to automatically channel IoT sensor data into a healthy data flow pipeline. From there, InfluxDB, a highly scalable time-series data provider, provides storage for structured data and data flows at an excellent level of detail, allowing for the analysis of historical sensor datasets. Then, Grafana visualises the data for display on dashboards and enables real-time monitoring and alerting for any substantive changes in the data, such as faulty operations for a device—node-RED acts as a data mediator, connecting sensors, smart contracts, and visualisation systems.

Figure (14) shows that the smart contract data is read with the Node-RED module. In the information node, the Node-RED module performs the rpcUrl and ABI of the already deployed contract and the call smart contract method. With the call, the data in JSON format is returned to the message payload.

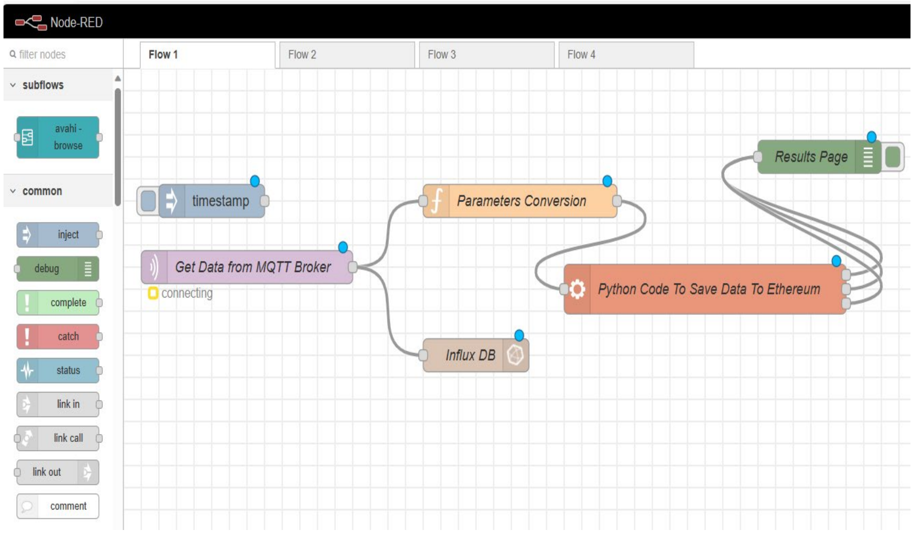


Figure (9): Nod-RED dashboard and function modules are used to transfer data from MQTT to Blockchain.

The data inserted in the smart contract in JSON format into the InfluxDB database is written with the Node-RED-contrib-InfluxDB package installed via the manage palette of Node-RED. In the information node of InfluxDB, server and database details need to be entered:

This data was stored in InfluxDB after the smart contract was read. Then, in Grafana, they built charts to display the collected data. Node-RED included the Grafana chart in the Node-RED dashboard via the "Embed Grafana Chart in Node-RED dashboard" flow and a custom Grafana dashboard. Likewise, the parsing and setting of the payload followed while the injection from InfluxDB took place. The Test Data Webhook was accessed to function as an endpoint, and that was all for the datasheet.

4.4.1 The Efficient Dynamics of Ethereum's Clique PoA Protocol in BCoT

The Ethereum PoA protocol forms the system's foundation, empowering designated authorities to function as signers (miners), actively mining and distributing blocks throughout the network. Upon the arrival of a new block, transactions undergo immediate verification, resulting in a network latency equivalent to a single block. At the heart of the system's efficiency and security is the Ethereum Clique PoA protocol, a robust consensus mechanism overseeing the operations of the Blockchain network. Notably applicable in IoT domains, it excels in handling real-time data with low latency. The protocol strategically designates trusted authorities to mine and distribute blocks, relying on the integrity of these authorised nodes, offering tangible benefits in network latency and power consumption.

The way the Clique PoA consensus works is that a group of vetted nodes participates in a round-robin process where individual nodes are responsible for creating blocks sequentially and in a fixed time interval. If a node cannot create a block during its turn, the next node in line creates it. Cycles of this nature give each authenticated participant an equal share of the block-production opportunity. If they successfully create a block, the node distributes the new block to all the other nodes in the network, which kicks off a series of transactions, where every node verifies blocks and then integrates them into the shared ledger. Apart from preserving the integrity of the Blockchain, this system also ensures that validators are incentivised to compete in a way that minimises their power.

In this way, the Clique PoA protocol demonstrates a very sophisticated balance between authority – through the nodes authorised in advance – and the decentralised execution of that authority, providing a robust, efficient, and scalable consensus mechanism for permissioned Blockchains (Rani, et al., 2023) (Islam, et al., 2022).

The Clique PoA protocol proves to be an exceptionally efficient consensus mechanism, facilitating swift and secure operations within the Blockchain network. Its inherent energy efficiency eliminates the need for resource-intensive mining equipment. Furthermore, the protocol seamlessly integrates into the IoT landscape, addressing resource constraints with low latency and minimal power consumption. The protocol's reliance on trusted authorities adds an extra layer of security, distinguishing it favourably from other consensus mechanisms such as PoW.

Getting data quickly is essential for remote control and immediate responses in IoT applications. In addition, power efficiency is where many IoT devices run on batteries, so saving power is crucial. Clique PoA is very energy-efficient, so IoT devices can use less power while staying connected. This is especially important for devices in hard-to-reach places. PoA is more secure than other methods like PoW. It relies on trusted authorities to make sure everything is safe. This helps keep the IoT network secure and trustworthy (Kaur, et al., 2021).

4.4.2 BCoT Security Analysis

The proposed architecture can measure Blockchain's impact on future IoT applications (in this specific application – for remote laboratories and machine learning-based real-time triaging of ICU patient vital signs), offering an extensive behavioural analysis of transaction throughput and latency, two crucial aspects of efficiency and scalability. The system comprises a CPS with three nodes based on the Raspberry Pi 4 model computing board. The nodes can act as authorised signers (miners) on a private Ethereum Blockchain using PoA consensus and smart contracts to create trust among the participants.

The architecture design also tackles indirect threats to the integrity of IoT apps, such as man-in-the-middle and Sybil attacks. Before these attacks can be executed through routing manipulation, double-spending, transaction malleability, cloning and other mechanisms, the intruder must access the network so that their malicious code is routed to the target microcontroller. With a private Blockchain and PoA consensus, this architecture network security is much improved. Second, there is an encrypted channel between all the nodes and the microcontrollers, so unauthorised routing modifications cannot be made. In the context of indirect threats inherent to Blockchain architectures, such as double spending, it is crucial for transaction validators to exercise rigorous due diligence. For instance, executing a double-spending attack requires the attacker to generate two transactions that indicate the expenditure of the same bitcoins. As the transactions are propagated around the Blockchain, these two invalid transactions will be marked as such, and whoever validates the transactions will know that they are coming from the same address and, hence, discard one of them. In this architecture, all transactions recorded on the Blockchain validated by selected signers and completed through smart contracts to make them immutable.

Second, application development stops the public risks associated with transaction malleability: smart contracts only enable and enforce standard, authorised transaction actions in their standard form, without any possibility for 'off-chain' modification. Cloning attacks are blocked with only authorised signers being part of creating and propagating the block, reinforced by the authentication system. The architecture is designed to recognise and avoid Sybil attacks by including authorised signers and options for additional identity authentication.

Furthermore, the system has a strong security indicator, which evaluates several crucial parameters of the network's performance, namely throughput, latency, and so on. RPi4 nodes have been additionally deployed to proudly prove the feasibility of the architecture in practice, delivering the desired level of security in IoT networks of remote laboratories. In addition, a built-in mechanism for continuous monitoring, regular security audits and implementation of best security practices makes it a robust architecture whose security can evolve to face new threats. Hence, the decentralised and immutable characteristics of Blockchain, augmented with the computational strength of RPi4 nodes and the safety of smart-contract execution, are proficient at providing the desired security, transparency and utility for IoT, which will enable novel and safe applications for IoT, enabling all levels – public and private – to benefit from IoT (Haque, et al., 2024) (Gulia, et al., 2024) (Allam, et al., 2024).

4.5 Chapter Summary

The integration of Raspberry Pi 4 (RPi4) nodes with an Ethereum PoA Blockchain, alongside various microcontrollers linked via MQTT, has been showcased as a powerful solution that provides numerous advantages such as improved security, enhanced communication capabilities, and greater automation. In this setup, an Ethereum PoA Blockchain was successfully deployed across three Raspberry Pi nodes, each interfacing with four microcontrollers through the MQTT protocol. The data generated by the sensors was systematically stored on the Blockchain and InterPlanetary File System (IPFS), utilising the functionalities offered by Node-RED. The selection of the consensus mechanism was tailored to meet the unique requirements of the Blockchain network and the edge processing strategies implemented to optimise system performance. As technological advancements continue, this integration is anticipated to evolve into more sophisticated applications, gaining traction within both scientific and engineering sectors. The architecture demonstrates the feasibility of combining these technologies and highlights the potential for future developments that could further enhance the efficiency and effectiveness of similar systems. The results indicate a significant improvement in operational metrics, suggesting that such integrations can lead to more robust and reliable systems supporting complex applications in various domains.

In the next chapter, Chapter 5: Blockchain as a Learning Management System for Laboratories 4.0, the chapter illustrates the evolution of the laboratory management system from Lab 1.0 to Lab 4.0. It describes a Blockchain-Based system for managing the remote lab, benchmarks traditional systems, and discusses the results and implications of the novel approach. The chapter describes the potential of Blockchain to revolutionise laboratory management.

Chapter 5

Blockchain as a Learning Management System for Laboratories 4.0

5.1 Introduction

At the beginning of the 21st century, the world witnessed the emergence of modern technologies that enabled it to identify the Fourth Industrial Revolution. It appears that this new revolution has turned the Earth into a site of excitement, uncertainty, and anticipation with a mixture of enthusiasm and fear. The new revolution has mixed the physical, digital, and biological worlds into one in a way that had not been achieved before. At its core, AI, Robotics, IoT, 3D Printing, Drones, Cloud Computing, Augmented Reality, Big Data, Blockchain, Nanotechnology and New Materials, Genetic Engineering, Quantum Computing, and other technologies are merging with and influencing the Internet. Mobile devices form a new CPS that would shape the future and profoundly impact individuals, industries, organisations, countries, and even international relations (Schwab, 2016). The Fourth Industrial Revolution will be a complex ecosystem of creative disruption, replacing old jobs and establishing lots of new categories of work. The shift will have far-reaching implications for the labour market ecosystem – and the skills needed for the workforce. The Fourth Industrial Revolution will lead to transformations in how we manage human capital, including how we develop leadership, transform organisations as consultants, and how organisations need to redesign the careers and job roles of their human workforce. With this wave of technological advancement comes a shift of old and new jobs; some positions in the workforce could become obsolete, while other new positions will develop. This will change the direction of work, requiring educational instruction and professional development systems to match the changes of working in Industry 4.0. Leadership models, consultation methods and hiring techniques must also adapt to this newly developed social and economic environment. The skills matrix required for employability in the new age is a widening array of cognitive and technical underlines the need for adaptive learning and agile career development to traverse the evolving occupational landscape of the Fourth

Industrial Revolution (Hirschi., 2018) (Michael A. Peters, 2016). To keep up with the new revolution, ministers and authorities worldwide are taking immediate action to follow the new era and introduce new technologies to provide better services, grow, and ensure a decent quality of life for their citizens (Ally & Wark, 2019) (Krajčo, et al., 2019).

A primary task for higher education institutions, particularly the universities, is to incentivise young graduates to be prepared for this new scenario to become a new creative generation in line with our industry 4.0, which is characterised by machines that are interconnected and can communicate with each other and collaborate day to day in the manufacturing and production industry. This summary of the vision of Industry 4.0 opens the door for establishing Education 4.0: Education 4.0 is a vision for the future of learning that reflects and motivates students' ways of life in which machines and humans can collaborate through a network to explore and innovate (Halili., 2019) (Hussin., 2018) (Xu, et al., 2018). Therefore, essentially, Education 4.0 is the vision, the blueprint of how learning is envisioned to be in the future and the preferred approach manner of learning, where students want a system that reflects and even improves their desired ways of living, and also the future of systems learning where machines can learn and perform joint tasks with humans across any given networks (networked learning) (Salmon., 2019). Because it should prepare engineers with the tools needed to deal with the management of digital technologies in a globally connected, technological world, Engineering Education 4.0 is the gateway to the vision of Industry 4.0, especially in this sense (Frerich, et al., 2016) (Coskun, et al., 2019). Indeed, the virtual and remote laboratories of today have made a significant contribution to crystallising and making more resolute a new paradigm of cyber-physical education that needs to monitor and control, through software algorithms and simulations, the physics experimentation of all the possible typologies and topics, as it becomes possible to connect the real with the virtual world (Auer, et al., 2019) (Mourtzis, et al., 2018). In contemporary distributed systems, Blockchain signifies a transformative paradigm for decentralised management. Such architectures facilitate the streaming and allocation of data to remote laboratories within a framework characterised by distributed, transparent, traceable, reliable, secure, and trusted peer-to-peer data sharing. This approach enhances operational efficiency and ensures robust data integrity and security, addressing critical challenges inherent in traditional centralised systems. By leveraging Blockchain technology, stakeholders can achieve improved accountability and trustworthiness in data transactions, fostering a more resilient infrastructure for collaborative research and development activities. Integrating these systems holds significant promise for advancing the capabilities of remote laboratories, ultimately leading to more effective and innovative applications across various domains. IPFS, an InterPlanetary File System that functions as a distributed storage, adds to this data ecosystem. It promotes a peer-to-peer hypermedia protocol capable of handling and storing the immense volumes of data stemming from operations in remote laboratories. The architecture of IPFS supports ways for 'sharing and storing' large datasets where integrity is maintained, and data accessibility is granted as these networks are spread out. The combination of Blockchain and IPFS technologies provides an elegant example of how data transfers can be secured and safeguarded for remote laboratory environments because of their unique characteristics of decentralisation, integrity and immutability, and also presents an attractive mechanism to transparently handle larger and larger volumes of scientific and operational data in scientific research settings (Hussein, et al., 2023).

5.2 Blockchain, IoT, and Education

5.2.1 Blockchain in Education

Blockchain technology has been viewed by universities in various parts of the world as having immense potential. It has led to various possibilities from when its scope was simulated for adoption into our world. Published works on Blockchain in education started showing up in literature, with each year seeing an increased number of publications all focusing on Blockchain applications in different areas of education, as explained by other researchers. Various reviews then were published on Blockchain and education; however, up to now, all of them have practically illustrated how Blockchain has been received in education to promote the opportunity of its implementation and the palatable effects it can bring to education. These surveys highlight the trajectory of Blockchain into many applications in higher education institutions, all geared toward improving teaching and learning activities and enhancing collaboration among stakeholders – students, teachers, parents, and potential future employers (Atienza-Mendez & Bayyou., 2019).

In addition, Blockchain may play a significant role in four strategic scenarios: identity and students' records, cost, and new pedagogy (Sahonero-Alvarez, 2018). These are ten features of Blockchain: distributed consensus, transaction validation, innovative contract platforms, peer-to-peer value transfer, incentive, bright property, security, immutability, uniqueness, and smart contracts. Decentralised Blockchain has been witnessed to attract university administrations and processes, including e-transcripts and digital degrees verifying and sharing certificates, assuring reliability, competence demonstration and learning outcomes management, reviewing the student's professional ability, fees and credits transfer, test review, cloud storage for personal information, identity management, and functioning a blended or distance learning and lifelong learning.

Reis-Marques et al. speculate that Blockchain technology 'could bootstrap learning with equal incentives', citing how the 'magic' of the Internet had been lost and that people focused on securing content and sharing knowledge. Attention was turned toward creating safe, cognitive virtual learning zones for stimulating learning (Reis-Marques, et al., 2021). This attention could transform how professors provide lectures and content, administer the course, and access students' reports, assignments, and exams. However, despite its relevance, they note that Blockchain has never been applied in engineering education, with only a handful of literature contributions to the field, specifically in new pedagogy, CPS, and remote labs. At the same time, Kassab et al. noted the undeniable industrial need for Blockchain experts. They comment on the main qualities of the current job offers. Such innovations gave fresh impetus to calls for overhauling engineering education and reorienting it to focus on Blockchain-native software engineering at the bachelor's degree and other more practical specialised learning opportunities (Mohamad, et al., 2021).

Blockchain technology can revolutionise university life across education by upgrading user and system support and through automated procedures and checks, ensuring academic integrity using long-term logs, which are difficult to erase. For years, universities have attempted to classify their data into various categories. Blockchain will finally bring some logical standards to the process and allow management to transfer across all data types. Blockchain technology can accommodate most university requirements. For example, many institutions and businesses already rely on Blockchain technology, which helps facilitate academic procedures and processes on a digital platform and aligns management standards.

Blockchain technology existed before its introduction into education, but that name did not refer to it. Indeed, UC Nicosia started storing diplomas in Ethereum and receiving Bitcoin payments for study fees in 2014 (Castro & Yong-Oliveira, 2021). Moreover, MIT – which has a track record of technological breakthroughs (like the creation of the first programmable computer in the 1940s) – teamed up with a Machine Learning start-up to develop a Blockchain cohort known as Blockcerts, geared towards 'making it straightforward for anybody to issue and verify open, Blockchain-backed diplomas and academic certificates in 2016' (Castro & Yong-Oliveira, 2021). Quite a few articles found in academic literature posit the idea that Blockchain can be used in different domains, from certifying credentials to accrediting academic programmes and schools, for safeguarding educational management systems, safeguarding digital rights, student performance, learning outcomes, and more (Panagiotidis, 2022).

In early 2018, 13 professors (six from Oxford University) floated an intriguing new idea called 'Woolf: The First Blockchain University'. The white paper described a decentralised university model built on Blockchain technology, abolishing administrative 'middlemen', promoting faculty governance, and enabling smart contracts to guarantee transactional security. Meanwhile, the goal was to help solve the student debt crisis and the overdependence on adjunct professors by allowing for direct interactions between students and professors, eliminating overhead, and creating continuing revenue streams for educators. By the summer of 2019, Woolf had quietly abandoned its Blockchain emphasis and turned to a standard online learning platform, possibly because of regulatory and practical complexities in implementing the Blockchain model (Jandrić, 2020). The basic model of Blockchain University is that professors will be able to share what they have learned with potential students, offer courses and modules of courses, and, in the process, allow those students to accrue credit toward undergraduate degrees (Anon., 2018). The Blockchain University also includes tools that automate most of the transactional, administrative tasks – student enrolment, registration, billing, payment, certificates, letter grades, etc. – reducing overheads significantly (and replacing much of the need for orchestrators) and allowing for a purely decentralised, flowing, self-organising school structure in which individuals are the architects of their contractual processes.

Several Blockchain-based educational and learning-oriented commercial systems have been developed to serve students, universities, and employers. Some are specialised Blockchain-based certification and identity-management platforms such as Digital Credentials Consortium, Open-Source University, AP-PII or BCDiploma, while others, like BitDegree and ODEM.io, are more directly aimed at lifelong learning by promoting lifelong learners (Steiu, 2020). Meanwhile, Sony Global Education is a cross-sectional third-party assessment platform, released in collaboration with IBM in 2016, that purports to be a multi-functional global open-education infrastructure that supports multiple types of assessment, stores, protects and shares data on student performance and development information (Panagiotidis., 2022).

Gilgamesh is another new Knowledge Exchange Platform on Ethereum smart contracts, opening in 2022 in San Francisco, California. Readers of books, students and writers can all participate in dialogue with each other across all genres of writing. Participants can earn rewards through tokens as an incentive and are encouraged to contribute content, discuss it in writing, and buy more academic e-books. Another interesting example is the BEN, a community of students and alumni worldwide created by students from MIT and the University of Michigan engaged in Blockchain initiatives since 2015. BEN has more than 4,000 members and has a worth of $11 billion created through its ideas, prototyped, and launched start-ups (Anderlini, et al., 2023). Blockchain technology has enabled university library services to be more cooperative and efficient, creating a unified university innovative library network. (Li, 2022). Recently, a Blockchain-based innovative library scheme for intelligent value-added services was proposed to solve problems related to resource collection, data storage, and information dissemination (Hu, 2022). It also solves the Smart Library's security problems from data collection, storage and dissemination and improves the user experience.

Using the Blockchain technology on the hardware feature provides opportunities for networks to manage datasets to create data empires in the context of an intelligent university and ensure everyone, including faculty, students and other stakeholders, can access the system remotely but without accessing the raw data, therefore, maintain the confidentiality, integrity of data (Hou, et al., 2020)· The system design comprises four levels as follows: perception collection, backbone, management, and service such that resources coming from various sources, including educational administration system and public facilities; campus networks, smart terminals; and sensors can be connected to the system and record/capture the activities conducted by the student and teachers within the university. Recently, An Ethereum-based Blockchain has been proposed for implementation in the remote laboratory to safeguard the successful operation of online experimentation and the opening up of data and information transmission in a decentralised, open, verifiable, reliable, secure and trustworthy method, thus guaranteeing the privacy of student files and reports (Al-Zoubi, et al., 2022).

The uses mentioned above are just the beginning regarding Blockchain technology's benefits to colleges and other higher education establishments. The technology will take some time to fully develop and become apparent in practice, allowing its effects to be felt widely. However, Blockchain technology continues to be a serious contender for the "next big thing," which might transform higher education and usher in its next development phase.

5.2.2 IoT in Engineering Education

Today, in terms of the pace at which our lives are changing, modern technologies are entirely reshaping our daily living and work-based routines and habits, transforming whole fields such as education and higher education and impacting each person. Despite the many reasons why new technologies are reshaping education and universities, one of the most important ones is undoubtedly the impact of emerging technologies on the learning format (Abbas, et al., 2021). Online learning platforms such as Coursera and Udacity allow students to access learning from anywhere in the world for the first time, providing many students with opportunities they would never have had without these modern technologies. Other emerging technologies are also transforming aspects of learning. For instance, in terms of how students learn, AI is now being used to create bespoke learning experiences that match individual students, such that a machine can monitor a student as they are learning and assess when a student needs extra support, thereby allowing them to learn at their own pace and in a way that is most impactful for them (Popenici & Kerr, 2017).

IoT technology is an innovation that is helping to transform engineering education. It is an emerging technological revolution that takes the idea of connecting physical devices with digital platforms to the next level (Asad, et al., 2022). Regarding engineering education, IoT can help create smart classrooms and laboratories with intelligent sensors, cams, etc. Students can interact with different connected devices and systems to perform hands-on activities and gain a more practical understanding of the engineering subjects. Also, the IoT can enable remote monitoring and control of equipment. This can help students perform their experiments, gather data away from the lab, and make learning more flexible. As any of these technologies mature, they will likely continue opening up new learning possibilities, assisting students in preparing for future careers and supporting their success in the workplace. The implementation not only enhances accessibility but also allows for personalised customisation, thereby significantly improving the learning experience. However, it also makes learning more entertaining. For example, IoT provides an opportunity to simulate real problems in engineering (Košťál, et al., 2019), providing a hands-on approach to learning, engaging and immersing students in what they are learning, and helping them maintain a deeper understanding of abstract concepts and things they may otherwise have difficulty comprehending. Because emergent technologies are coming faster than ever, it is much easier for teams to build products, and new tech use will increase in the coming years. This also means there will be new opportunities and challenges to overcome. As emerging technologies develop, they will provide educators with new learning methods to equip their students with the proper skills to succeed in the demanding and growing job market.

Over the past years, universities and other institutions of higher education, in particular, have committed themselves to doing so by placing their training programs as well as research and development activities at the service of the new era through their vision to produce well-equipped graduates to face the complexity of the new era, including education 4.0 as well as innovation and creativity and agility for the impact of Industry 4.0 on the interconnection of the equipment, and able to face and manage productions and manufacturing processes (Halili, 2019). In line with Education 4.0's roadmap for future learning, students would experience learning practices that mirror and catalyse how they live in environments dominated by symbiotic networks of artificial and human intelligence interacting to innovate new dimensions of possibilities (Salmon, 2019). Engineering Education 4.0 is critical to actualising the vision of Industry 4.0, as it will enable educational institutions to produce engineers who can effectively harness the power of digital technologies in a technology-intensive and globally interconnected environment (Frerich, et al., 2016) (Coskun, et al., 2019). The establishment of the virtual, remote lab significantly influenced the description and representation of a new cyber-physical educational approach, in which physical experiments of various types and subjects are monitored and controlled by the software algorithms and simulations, increasing the dynamic interaction between the physical and virtual worlds, and becoming the core of the framework of Education 4.0. (Auer, et al., 2019)¸ (Mourtzis, et al., 2018).

Since the inception of Bitcoin in 2008, the introduction of Blockchain technology has gained momentum across multitudes of digital platforms such as cryptocurrency, finance, medical, logistics and charges. Nevertheless, education has shown a mediocre choice in using Blockchain for educational administration, including credential information management, competency and learning outcomes management, student professional competency measurement, fee and credit transfer, exam review and lifelong learning (Alammary, et al., 2019), (Vargas & Lindín, 2019), (Cheng, et al., 2018).

Blockchain technology has found applications in numerous emerging fields, one of the most significant being the IoT (Alkadi, et al., 2021). Its potential extends to CPLs to enhance the educational experience, Blockchain should be integrated into course management and laboratory operations, seamlessly connecting with the learning process through a middleware interface (Narasimhan, et al., 2003). In both cases, Blockchain could be leveraged as a remote CPL providing authorisation, authentication, and scheduling services to ensure exclusive access through a queuing service or access to a calendar-based access-reservation mechanism and user-tracking services. Blockchain could replace third parties such as an LMS and deliver all relevant theory documents and protocol tasks to the students, including any additional information they might need. Moreover, Blockchain could facilitate communication between students and instructors, making it a valuable part of the e-learning experience.

In CPL-based Blockchain environments, the students can use the username and password to connect to the CPL, book a specific timeslot, open a specified web page for controlling the remote experiments as per the manual, get readings and adjust measurements, and visualise the different variables. At this stage, students may save the experiment results and put the acquired data in a file repository in the Blockchain; the laboratory reports are used to author the final reports, and then the submitted reports can be sent to the lecturers. This, in turn, means that CPLs can, in the future, be adapted to work in conjunction with exotic distributed systems without impairing the ability to read, store and synchronise data across devices via a cloud storage solution (Llanos Tobarra, 2016).

5.2.3 Blockchain and Engineering Education 4.0

The seamless integration of CPL and Blockchain Technology into Education 4.0 allows graduates to interact with the customised technical knowledge that engineering and allied professionals are expected to develop for the world in the new multi-dimensioned interconnected environment of Industry 4.0.

Moreover, CPLs with the Blockchain platform offer hands-on learning experiences at a human-centric level of interaction. This facilitates designing complex engineering courses and real-world problems that can be explored through socially immersive simulations and ready-to-use physical labs and machines. The essence and core of Blockchain for decentralised training in CPL ecosystems is that it provides a secure-shared-ledger for courses, content and lab resources management in smart labs and e-learning environments by enabling three critical services: authorisation, authentication, and scheduling of students. To experience hands-on learning via virtualised physical and digital lab environments for realistic learning by doing, students must be authorised to create virtual and physical accounts to access the labs and machines using queuing/reservation-based strategies (Al-Zoubi, et al., 2022).

By accessing the experiment's peripherals remotely from their laptop or mobile device in a CPL Blockchain environment, the students can configure the apparatus, alter inputs, take readings, and commit the data dynamically to a repository independent of the experiment to which it is related. The Blockchain enables this data collection to be transparent, auditable, and unalterable.

In the lab of the future, systematic integration with IoT and Blockchain is carried out as a layer within the CPL system architecture. While the approach will soon potentially revolutionise many engineering laboratories, several barriers remain. Security, connection, and performance are all important, often challenging, issues that must be addressed. Nonetheless, the combination of Blockchain and IoT technologies within CPLs has enormous potential to set a new standard for engineering pedagogy, closely aligned with the vision of Education 4.0, and prepare the next generation of engineering students to thrive in the digital era (Al-Zoubi, et al., 2022).

5.2.4 Moodle as a Remote Lab Management Solution

Technology-based learning is a model already undertaken by highly developed countries and introduced as an intrinsic part of those local educational systems and curricula. Also, in the engineering eLearning context, engineering learning materials and educational resources require developing specialised components for education and training (Gonschor, et al., 2022). Remote laboratory experiments allow students to research how actual equipment works and apply the theoretical concepts previously learned from classroom models. Consequently, experimentation is an integral part of engineering education. So, a university that prides itself on offering this kind of teaching must consider the learning laboratories as an integral part of its teaching model. Experiments in remote online laboratories became obligatory for creating renewable-energy learning scenarios. Instead, remote laboratories became the tool of choice for teaching all the concepts concerning renewable energy. One could say that higher education is moving towards a trend where, every day, new experimental sites enrich the traditional teaching strategy consisting of in-class lectures and hands-on laboratory classes (Monaco, et al., 2012). Although the theoretical part of the college pupil’s curriculum could be partly covered by the educational resources that the Internet provides for creating theoretical frameworks, in some fields of study, especially those related to engineering and sciences, there is an even more severe problem: a necessity to build, if not wholly, then at least partly the practical part of the content of their courses by using Internet-based technologies and tools.

In the last decade, digital educational media has been used increasingly in distance education. Nowadays, we can observe that using digital media positively influences the students' knowledge, competencies, and attitudes, influenced by the rising number of tools provided for teachers and educators, such as LMS or Web-based laboratories. LMSs are the engine of administrative, documentation, monitoring, and reporting services for training or course programmes – whether online or presented ‘live’ or in the workplace. Developed over several decades and refined over years and sometimes decades, they serve as a sophisticated infrastructure supporting the content management, communications and tracking of learners and their progress. The theoretical bases can be taught – and for some subjects, such as many humanities and sciences – through online materials. However, the practical side of most vocational education (such as engineering and science) requires new forms of application that take advantage of internet-based tools, such as Web-based laboratories and simulations (Wuttke, et al., 2019). Web-based laboratories refer to platforms that mimic or demonstrate scientific phenomena that require expensive or time-consuming equipment and should consist of two distinctive and complementary components:

1. Virtual Laboratories provide computer-based simulations with views and manipulation options similar to original simulations. In recent years, various existing simulations have been reinvented, involving interactive graphical user interfaces (GUI) where students can manipulate the experiment's controls and observe its development.
2. Remote labs use real-world equipment, not simulations, to introduce students to practical work. The equipment is accessible online, allowing students to interact in real-time. This method of conducting experiments remotely via the Internet began over ten years ago and has continued to grow ever since. Initially, a group of European projects assessed the quality of labs and determined which experiments were necessary by analysing the university's curriculum. Subsequently, specific experiments were selected and available across multiple labs at the College of Engineering. This enabled students to engage in engineering experiments remotely at the university level, enhancing the educational process.

Experimental design researchers also led the way in creating the protocols that guide experiment design, establishing the proper approaches for industry to build labs, and setting the academic agenda for what should be made possible by experimentation. In tandem with the emergence of visions of the future of remote labs were the companies whose purpose was to build them. Companies with experience in engineering design and development created course-specific, experimental remote laboratories for engineering departments to support disciplinary laboratory offerings. The experiments to which students had experiential access were predefined. Students were allocated scheduled time slots for these remote experiential learning activities. The resulting data would then be collected by web services or written into local files on the computer. So, the students could access this data to perform data processing—the universities where these laboratories existed, or the students that used them all existed in various places. Internet connectivity allowed these laboratories, which are physically distributed worldwide, to function like such. The cameras enable a real-time video broadcast so that students can watch the procedure when it is running. The laboratories were connected as in Figure (5).

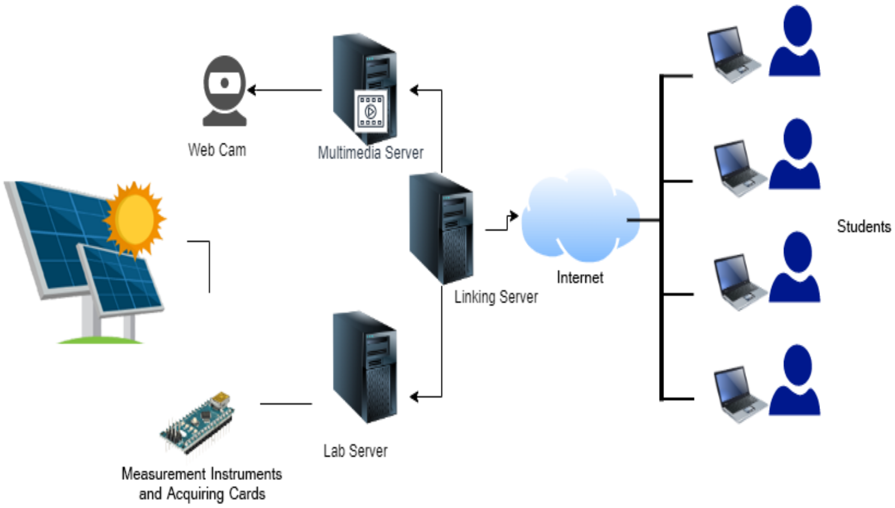


Figure (10): General architecture of remote labs.

This remote lab teaching system uses Moodle as a software package. Moodle is a free, open-source software package for course management systems and virtual learning environments. Moodle uses free, open-source code to establish Internet-based courses and websites. It has all functions implemented by the modules, which include site management, user management, course management, task modules, selecting modules, chat room modules, forum modules, logging modules, test modules, resource modules, and other modules which can be integrated and applied to the course design. The Moodle learning management system is built upon a robust technological framework comprising various components, including web servers, databases, programming languages, and operating systems. At the core of this architecture lies the Apache HTTP Server, the predominant web server powering a significant portion of internet traffic.

Apache, an open-source software, has garnered widespread adoption due to its accessibility and collaborative development model, involving a diverse global community of individuals and organisations. Despite its open-source nature, Apache has proven its reliability, flexibility, and extensibility, making it a highly scalable solution capable of handling high-traffic websites.

The software's stability, cost-effectiveness, and open-source codebase contribute to its compatibility with numerous computers operating systems, enabling seamless installation and deployment across various platforms without restrictions. The latter's free and open-source licensing model facilitates Moodle's integration with Apache as its web server.

Complementing the web server component, Moodle utilises MySQL, a fast, reliable, and open-source database management system. Efficient query processing is a critical aspect of database performance, and MySQL's optimised indexing and rapid search operations have made it a preferred choice among Internet companies and significant organisations.

Moodle's selection of MySQL as the default database is further reinforced by its seamless integration with Apache and PHP, forming a cohesive technology stack that operates efficiently across multiple operating systems. PHP, a server-side scripting language, is renowned for its cross-platform compatibility. It supports various operating systems, including Windows and UNIX-based environments and web server systems. This versatility enables Moodle, a PHP and MySQL-based application platform, to run seamlessly across diverse operating systems, contributing to its widespread adoption and flexibility.

As a teaching solution, Moodle is chosen. Its extensible interface (i.e., plugins) will provide a component architecture for adapting some functionality. It provides an activity module that enables a connection with remote laboratory services. This kind of technology is very different from other LMS. The laboratory will be considered in its structure of a group of services (LaaS), so we do not have to integrate it into the complete module form. This increases the adaptation of laboratory system options from a component perspective, creating lightweight adaptive laboratories and increasing flexibility. The plugin will make up the standard generic functionality of the Moodle platform. However, it can automatically register laboratories. Then, it will provide an opportunity to accept the creation of an experiment. It will also connect the remote laboratory with the plan of the course of work. For instance, it will offer a chance for students to master their capabilities, which will complement the training activities.

When such tools are embedded into the learning process in a distance learning paradigm, say in the remote laboratory in the renewable energy area, such a set of characteristics might impact more than one dimension, such as the curriculum plan and the workflow (and the progression of students' work) in the online courses presented in the distance. Renewable energy education's transition to distance learning necessitates significantly adapting traditional teaching methodologies. The highly structured and meticulously designed online course format becomes imperative, as it facilitates the effective delivery of educational content remotely. Furthermore, developing novel instructional materials tailored to guide students in leveraging embedded resources is crucial. Teaching strategies and curricular content developed for remote learning environments differ substantially from those employed in conventional classroom settings. This paradigm shift necessitates a comprehensive exploration of the interplay between distance education's unique characteristics and their impact on learning outcomes. Investigating approaches to enhance output quality and optimise the effectiveness of remote pedagogical approaches emerges as a critical area of inquiry. Moodle, a widely adopted LMS, is built upon the PHP programming language. Its core functionality is driven by a PHP process running on a web server, which interprets PHP pages requested through URLs and executes the corresponding code. Proper installation and configuration of PHP on the web server are essential prerequisites to leverage Moodle's capabilities. Moodle's permission system is role-based, assigning users specific roles within different contexts. The combination of roles and contexts determines the user's permissions and access levels on each page. A typical context within the Moodle ecosystem is a course where roles and permissions are defined and managed accordingly.

On the other hand, with LabVIEW, an application was proposed (Hammad, et al., 2020) dedicated to designing a virtual lab for instrumentation/measurements. The described system accomplished the function simulation and stored the acquired data in a Blockchain private wallet, i.e., a Private Wallet. Moreover, current attempts are moved to create an innovative security solution for the implementation of FPGA remote labs, following a joint project between the Universiteit in Montreal (Montreal, Canada) and the Universidade do

Futebol Clube de Sao Paulo for the development of a working platform providing standardised security procedures through the implementation of Blockchain technology, aiming to develop a safe and easy-to-use Ethereum-based control system using an extra authentication and authorisation layer to improve robustness of the security level of remote experiments (Zet & Dumitriu., 2021). Another solution proposes developing and integrating Moodle with Ethereum to utilise Blockchain applications, integrating big data technologies (Werner, et al., 2021). A performance analysis was carried out in a dedicated paper to test the proposed solution in different usage scenarios. Further, e-learning frameworks with an integrated LMS to protect the university-distributed repository (Morais, et al., 2021) were also empowered how to implement the materials, questions and assessment banks to securely store the certification validation receivable at any part of the world versus the main aim to implement a distributed large-scale system according to a perspective to the private Blockchain model written in PHP language and implemented on Google Firebase (El-dosuky & Eladl., 2019). The examples above reproduce the central Blockchain-LMS lab 4.0 and offer the opposite of the above-stated effort to embed the Blockchain in technology-mediated learning.

5.2.4.1 Remote Lab Virtual Learning Environment

Implementing remote laboratory facilities at the university involved a comprehensive development, testing, and integration process. The web-based interfaces for these remote laboratories were hosted on the institution's primary servers, and a diverse cohort of students conducted a series of rigorous experiments to validate these laboratories' functionality and ensure the generated data's accuracy and comprehensibility. Upon successful completion of the laboratory and experimental validation process, the facilities were made accessible to the student body. Since the current experimental setup necessitates individual student access during designated time slots, implementing a specialised platform for managing student access became imperative.

Following an extensive evaluation of available platforms capable of providing the required functionality, the institution opted to utilise the Moodle virtual learning environment (VLE) as the primary platform for organising and facilitating student access to the remote laboratories. This decision was informed by Moodle's robust capabilities as a Learning Management System (LMS) and its potential for seamless integration with the remote laboratory infrastructure. The VLE was developed as a comprehensive eLearning delivery mechanism, not only for the remote laboratories but also for other courses within the curriculum. Careful consideration was given to selecting appropriate VLE tools for designing and adapting various eLearning courses, including those focused on photovoltaic and renewable energy technologies. The implementation of Moodle as the LMS within the VLE framework involved the incorporation of specific plugins and additional software tools to manage task queues, laboratory bookings, and scheduling systems. Particular attention was paid to integrating remote laboratories with the VLE to ensure a cohesive and user-friendly experience for students and instructors.

The technical specifications of the VLE implementation included Moodle version 2.4.3+, PHP version 5.4.7, and MySQL version 5.5.27. Three distinct account types were established to facilitate effective administration and usage of the system: manager, instructor, and student. The entire VLE infrastructure was deployed on a dedicated server to ensure optimal performance and reliability. Although students can improve their learning experience by establishing a remote lab without many resources, setting up a small-scale lab for just one experiment with a lecturer's help is not enough. The instructor must determine the best way to expand the lab successfully while dealing with issues like security, stage growth, blending different subjects smoothly, guaranteeing accessibility, and preserving the lab's operational reliability. The aim is to develop a remote lab setting that promotes various innovative experiments, allowing students to investigate and test independently while enjoying an immersive and captivating learning journey.

The prototype of a remote laboratory has been developed to illustrate its potential. The first phase of the prototype's development has been described. Furthermore, the partners have expressed their opinions and questions concerning the prototype's development, network bandwidth restrictions, user security, and potential integration into a course. This is the first step in determining the services of additional integration of remote laboratories.

Therefore, for the remote laboratories to be federated, they must have the following additional services:

- User creation and authentication are handled directly by the Moodle platform.
- A booking system for remote laboratories must be developed.
- Concurrent access for remote laboratories, which must be built.

- Authorization, which is provided directly through the VLE Moodle.
- A video streaming server is accomplished using Webcam IPs installed in the physical laboratory.
- The Moodle platform and the laboratory services provide user monitoring.
- Given priority to concurrent access and booking system options.

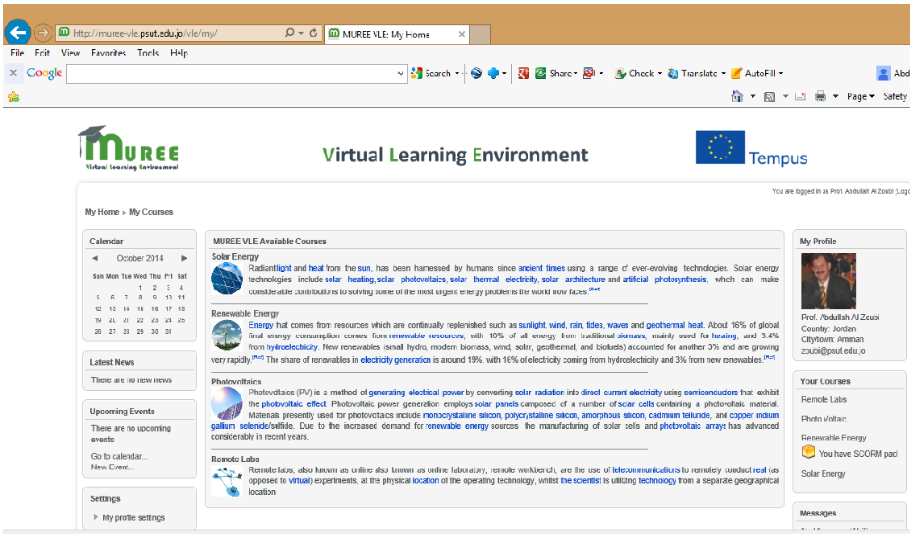
By sharing laboratory installations in their courses, institutions do not have to duplicate the deployment of identical laboratories at each institution. This avoids many costs and provides students with a global and more diverse range of labs. Thus, remote lab repositories would be created rather than just providing isolated remote laboratories managed by RLMS middleware, such as WebLab, DEUSTo, LabShare SA, Related, or LiLa. Such software can provide most missing services to remote laboratories and usually offers concurrent access and scheduling schemes.

5.2.4.2 Experiments of Remote Lab

One of the primary objectives of the e-learning course and the renewable energy laboratories is to enforce the educational innovation practices employed in distance education settings. Furthermore, the LMS facilitates the delivery of theoretical online classes by integrating features and tools such as administrative, synchronous, and asynchronous communication capabilities, assessment and monitoring capabilities, multimedia sharing capabilities, and standardised compatibility. The LMS conducts learning in online courses.

5.2.4.3 Courses and Experiments Material

The suitable educational and teaching materials were chosen, and attention was paid to integrating the remote labs developed into the VLE so that both the courses and remote labs deliver full interactivity and provide flexibility in content delivery and the possibility of shared social learning across partner institutions. All the materials required for renewable energy systems eLearning courses to deliver the traditional content were prepared and designed, as shown in Figure (6).



http://muree-vle.psut.edu.jo/vle/my/
MUREE VLE: My Home
File Edit View Favorites Tools Help
Google
Search
Share
Check
Translate
AutoFill
Page
Safety
MUREE Virtual Learning Environment
Virtual Learning Environment
Tempus

You are logged in as Prof. Abdullah Al Zoubi (Logo

My Home ▸ My Courses

Calendar

◀ October 2014 ▶

Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Latest News

There are no new news

Upcoming Events

There are no upcoming events

Go to calendar...
New Event...

Settings

▸ My profile settings

MUREE VLE Available Courses

Solar Energy

Radiant light and heat from the sun, has been harnessed by humans since ancient times using a range of ever-evolving technologies. Solar energy technologies include solar heating, solar photovoltaics, solar thermal electricity, solar architecture and artificial photosynthesis, which can make considerable contributions to solving some of the most urgent energy problems the world now faces.[Ref]

Renewable Energy

Energy that comes from resources which are continually replenished such as sunlight, wind, rain, tides, waves and geothermal heat. About 16% of global final energy consumption comes from renewable resources, with 10% of all energy from traditional biomass, mainly used for heating, and 3.4% from hydroelectricity. New renewables (small hydro, modern biomass, wind, solar, geothermal, and biofuels) accounted for another 3% and are growing very rapidly.[Ref] The share of renewables in electricity generation is around 19%, with 16% of electricity coming from hydroelectricity and 3% from new renewables.[Ref]

Photovoltaics

Photovoltaics (PV) is a method of generating electrical power by converting solar radiation into direct current electricity using semiconductors that exhibit the photovoltaic effect. Photovoltaic power generation employs solar panels composed of a number of solar cells containing a photovoltaic material. Materials presently used for photovoltaics include monocrystalline silicon, polycrystalline silicon, amorphous silicon, cadmium telluride, and copper indium gallium selenide/sulfide. Due to the increased demand for renewable energy sources, the manufacturing of solar cells and photovoltaic arrays has advanced considerably in recent years.

Remote Labs

Remote labs, also known as online also known as online laboratory, remote workbench, are the use of telecommunications to remotely conduct real (as opposed to virtual) experiments, at the physical location of the operating technology, whilst the scientist is utilizing technology from a separate geographical location

My Profile

Prof. Abdullah Al Zoubi
Country: Jordan
City/town: Amman
zoubi@psut.edu.jo

Your Courses

Remote Labs
Photo Voltaic
Renewable Energy
You have SCORM pacl
Solar Energy

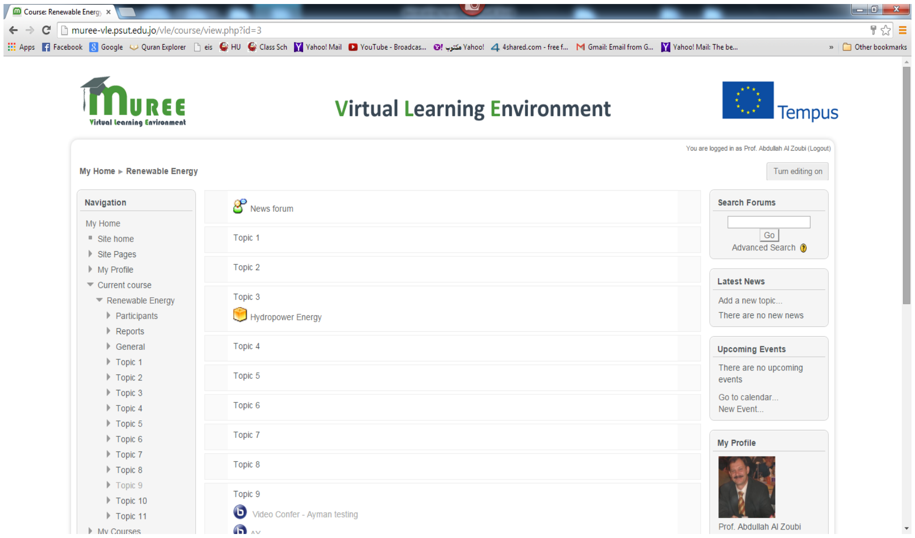
Messages

Figure (11): Page of eLearning courses and remote labs.

The content of the courses was developed. An assessment and evaluation strategy were also developed to adapt the materials to the VLE platform. IT tools such as Moodle virtual learning environment, Adobe Photoshop and Flash for image editing and creating animations, and Lectora publisher for the content authoring tools were used. The courses were structured into topical modules, with each chapter packaged into the Shareable Content Object Reference Model (SCORM) format, adhering to a maximum upload size of 80 MB. This approach facilitated the seamless integration of the chapters into their respective topics within the learning management system.

A comprehensive development process was undertaken for each chapter. The initial phase involved defining the chapter outlines and learning objectives and conceptualizing the overall design and layout. Storyboards were meticulously crafted to guide the content creation process. Multimedia elements, including images and animations, were carefully curated, and edited to enhance conceptual clarity and foster interactivity. Narrative sound files were recorded for all pages and animations, ensuring an immersive and accessible learning experience for diverse learners, including those with disabilities. The e-learning content was assembled within the Lectora authoring environment, where all components – textual, visual, auditory, and interactive – were seamlessly integrated into a cohesive and engaging learning experience. The chapters were subsequently organised into thematic sections, with the photovoltaic course comprising seven sections: sun, silicon, solar cell, grid-connected systems, stand-alone systems, design of stand-alone photovoltaic systems, and their economic considerations. Concurrently, the hydropower energy course spanned ten sections, encompassing a statistical context overview, critical components of hydropower plants, system types, turbine selection and designs, technical issues, economic overview, environmental assessment, and hydropower applications.

Quizzes and tests were strategically embedded within the chapters to reinforce learning and assess comprehension. Upon completion, the chapters were published in the SCORM 1.2 package format and seamlessly integrated into the Moodle learning management system, ensuring a consistent and standardised learning experience across multiple platforms.



You are logged in as Prof. Abdullah Al Zoubi (Logout)

There are no new news

There are no upcoming events

Figure (12): Snapshot from Moodle after uploading the material: main topics.

5.2.4.4 Laboratories Web Services Development Description

The laboratories connected with the university's internal network, and each laboratory was given its IP address to facilitate access to it and connect it with the primary servers at the university. Web pages have been designed for each experiment. These pages contain tools to control the experiment remotely, a section for the webcam, and a section for data obtained from the laboratory. In contrast, the student controls it, as shown in Figure (8). These data are displayed in different forms or can be downloaded. This data is at the end of the experiment through the save buttons on the page.

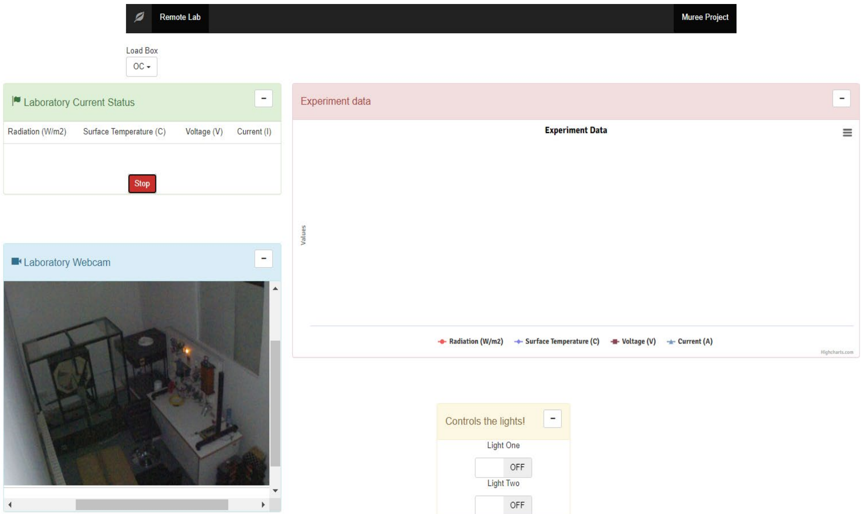
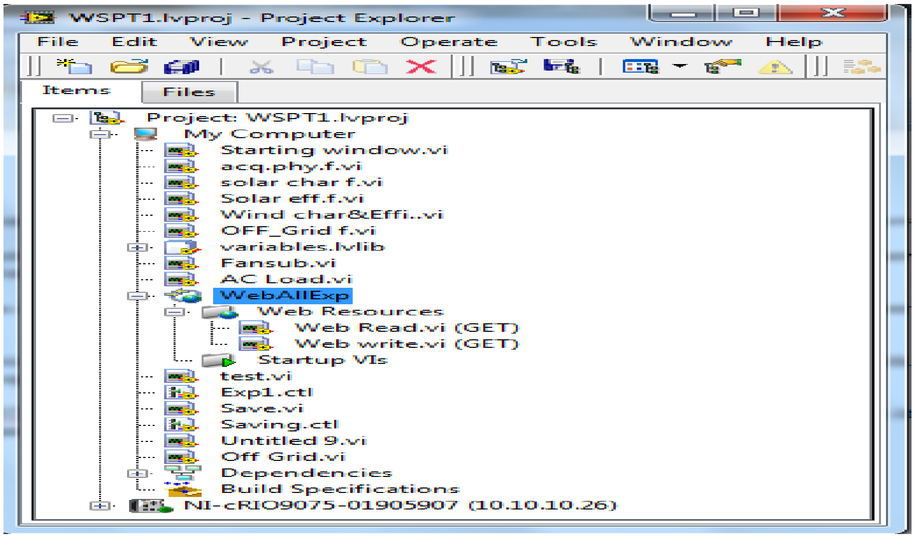


Figure (13): Screenshot of renewable energy remote experiment.

The concept of a Web service is based on the idea that two electronic devices interact over a network through a Web service. The software framework is designed to facilitate interoperable machine-to-machine communication over a network and provide a function over a network address via a Web service with the service always running, similar to the utility computing concept. To organise and configure the Visual Basic for Applications (VBA) and other files composing the Web service, a Web service is created in a LabVIEW project and published to the host computer, as shown in Figure (9).



```
Project: WSPT1.lvproj
  My Computer
    Starting window.vi
    acq.phy.f.vi
    solar char f.vi
    Solar eff.f.vi
    Wind char&Effi..vi
    OFF_Grid f.vi
    variables.lvlib
    Fansub.vi
    AC Load.vi
    WebAllExp
      Web Resources
        Web Read.vi (GET)
        Web write.vi (GET)
      Startup VIs
    test.vi
    Exp1.ctl
    Save.vi
    Saving.ctl
    Untitled 9.vi
    Off Grid.vi
    Dependencies
    Build Specifications
  NI-cRIO9075-01905907 (10.10.10.26)
```

Figure (14): Screenshot of LabVIEW web service.

5.3 Traditional Remote Lab Data Management Systems

According to this methodology, the backbone of traditional remote labs architecture is based on a client-server architecture supported in a shared system through different integration options and approaches, mainly login access, file resources sharing, indexing skills and experiment running. Major integration options include dashboards, VLEs, and grid technologies (Tobarra, et al., 2015) (Danilo, et al., 2009). Moodle is the most popular open-source platform, and it is widely used as a learning management system (LMS) to provide students access to lab hardware (Guinaldo, et al., 2013). In Addition, Moodle contains some features, especially its ease of use for a large community of users and availability of tools for activities like administering, monitoring, and accommodating remote hands-on lab sessions. The platform runs on an open-source Apache web server based on PHP language and MySQL database. The platform supports a variety of plug-ins along with other software tools for electronic content management, virtual classrooms, assignments, and submissions and grading with associated feedback forms, quizzes (which allow the creation, delivery, and grading of online tests and quizzes), examinations, activity queues, lab booking (also called booking lab time/slots for experimental activities), online experiment scheduling (also called scheduling experiments at suitable time/slots for online tests), and submission extension mechanisms (Tobarra, et al., 2016).

These physical devices are generally located in devoted laboratories on college campuses, but remote students can control them through the Internet. The typical architecture of such remote labs commonly uses two servers: (i) one server to control the lab apparatus and (ii) another for connecting the setup to the internet. Typical architecture of a remote lab. A third server can be implemented to host multimedia tools. The linking server acts as the communication layer between the remote lab and the web clients, and it sends back to the clients the experimental parameter values and the sensor readings (or others) to fulfil all the client requests. The linking server fulfils the acquisition and control loop tasks. Furthermore, the laboratory deployment includes an IP webcam pointing towards the apparatuses to bring the environment to life. Generally, this is driven by the desire to give the students real-time visual images of the lab environment and provide some visual feedback.

The Moodle VLE server hosts the software applications of remote lab clients itself, such as the operation procedures required for the management and arrangement of the students' connections with the experiment; the information is processed in a selected web service due to its universal technology, platform interoperability, unobtrusive nature and low bandwidth the graphical user interface (GUI) was written through the Java programming language, the HTML programming language, the CSS programming language and the web service technology. The GUI aimed to develop interactive simulations for pedagogic purposes and academic learning. In the GUI programming, three simple RESTful Web services were selected (Llanos Tobarra, 2016). The first one was defined for the lab instruments and hardware. The second one was sending data from the lab's significant sensors. The third one was defined to monitor the status of the laboratory. RESTful Web Service makes maintaining AJAX requests accessible through any website or programming language. As a result, data are sent in JSON rather than XML format to cut down the required bandwidth when transmitting information. In principle, with the help of Moodle, it is easy for administrators to have a seamless experience in organising, documenting, tracking, and reporting remote experiences. Moreover, teachers can provide a complete online learning solution, including running experiments with relatively simple management and interaction (Hammad, et al., 2020).

The VLE administrator sets up scheduling plugins, defines the laboratory name, examines the corresponding experiments, rejects the ineligible experiments, accepts the eligible ones, enrols the concerned students, registers student data in Moodle, and enables the student to conduct remote laboratory experiments by grouping all the allowed examples under one activity. Second, the administrator creates an experimental activity module, defines the parameters for the experiments, monitors the students through this activity, then defines the free time slots, where the environment is set up to let the student conduct the experiment written by the administrator, book a free time slot, click on the table that consists of all the experiments available. It creates a window containing all the free time slots available for that experiment. The flowchart of the selection process is shown in Figure (15). This scheduling system was developed and is used in developing ergonomics to help the students book the free time they desire without waiting for a spare time slot. The system automatically calculates the number of sessions permitted by the date based on the experiment's limitations.

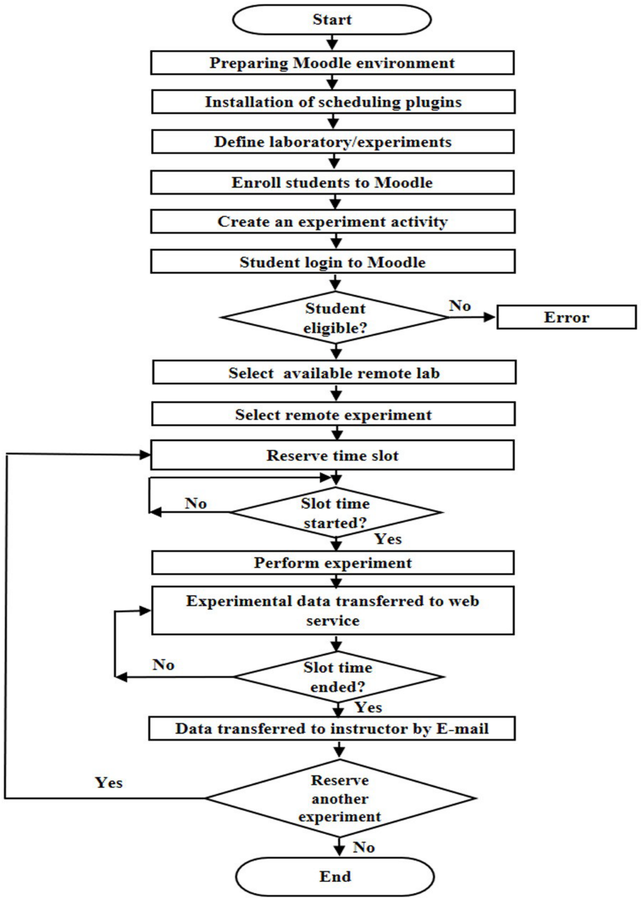
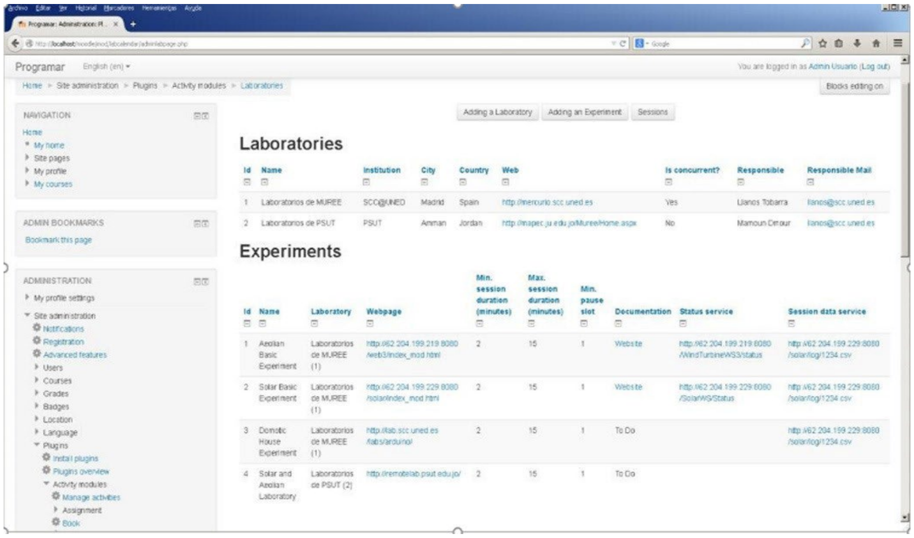

Start
Preparing Moodle environment
Installation of scheduling plugins
Define laboratory/experiments
Enroll students to Moodle
Create an experiment activity
Student login to Moodle
Student eligible?
No
Error
Select available remote lab
Select remote experiment
Reserve time slot
No
Slot time started?
Yes
Perform experiment
Experimental data transferred to web service
No
Slot time ended?
Yes
Data transferred to instructor by E-mail
Yes
Reserve another experiment
No
End

Figure (15): Flowchart of design of the Moodle platform.

The scheduling plugin shows the tables with the lab correlations and the experiment-saver controls, as shown in Figure (16). Three functions have been attached to the top of the admin page. A new lab is added by opening the Moodle registration form, as shown at the top of the admin page. This is the first step when the admin adds a new experiment for Moodle. Second, there is a facility to submit an additional experiment to the platform by opening another form to insert information about this experiment. Finally, let the administrator see a table and monitor the session state to review all plugin activity. The session page lists stateful work like waiting, running, completed sessions, time-out or unused, and an opportunity to drop the session. This value-added function is a hand if the activity is no longer relevant to the course. Thus, the admin can collect session information for the lecturer. On the other hand, the system is controlled by plugins for concurrency, as it allows only one sit for an experience at a time.



Laboratories

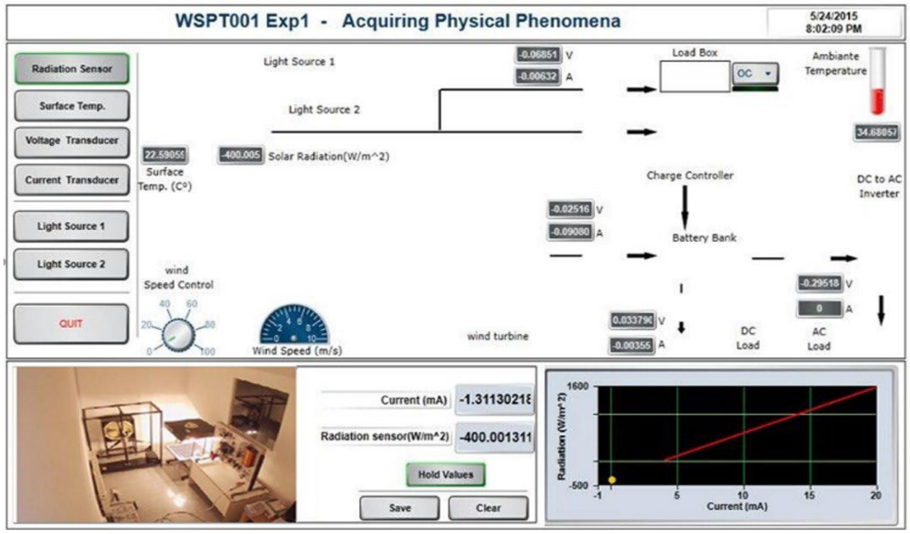
Id	Name	Institution	City	Country	Web	Is concurrent?	Responsible	Responsible Mail
1	Laboratorios de MUREE	SCC@UNED	Madrid	Spain	http://mercurio.scc.uned.es	Yes	Llanos Tobarra	llanos@scc.uned.es
2	Laboratorios de PSUT	PSUT	Amman	Jordan	http://mapec.ju.edu.jo/Muree/Home.aspx	No	Mamoun Drrour	llanos@scc.uned.es

Experiments

Id	Name	Laboratory	Webpage	Min. session duration (minutes)	Max. session duration (minutes)	Min. pause slot	Documentation	Status service	Session data service
1	Aeolian Basic Experiment	Laboratorios de MUREE (1)	http://62.204.199.219:8080/web3/index_mod.html	2	15	1	Website	http://62.204.199.219:8080/WindTurbineWS3/status	http://62.204.199.229:8080/solar/log/1234.csv
2	Solar Basic Experiment	Laboratorios de MUREE (1)	http://62.204.199.229:8080/solar/index_mod.html	2	15	1	Website	http://62.204.199.229:8080/SolarWS/Status	http://62.204.199.229:8080/solar/log/1234.csv
3	Domotic House Experiment	Laboratorios de MUREE (1)	http://lab.scc.uned.es/labs/arduino/	2	15	1	To Do		http://62.204.199.229:8080/solar/log/1234.csv
4	Solar and Aeolian Laboratory	Laboratorios de PSUT (2)	http://remotelab.psut.edu.jo/	2	15	1	To Do		

Figure (16): Remote lab scheduling plugin administration view.

The student directly goes to the experiment page to experiment. At the beginning of the session, a unique window pops up with documents and services, such as experiment descriptions, instruction sheets or manuals, slide presentations to be streamed by webcam, the equipment, and the webpage URL link where hardware configuration is carried out. The experiment returns a URL link to the web page displaying the experiment's status, such as hardware errors and the students who are already running if any experiments are being run. The link to the web service allows experiments to download a file, including the session's results and the session’s minimum and maximum length. The administrator sets these time limitations to configure the experimental session in courses. Also, the administrator can create an optional pause duration between experiments with a minimum duration for each laboratory, which the instructor can change. Finally, a timer is available to give the students an indication of the time remaining in the session. A button is available for the students to download student experiment data. A copy of the data will also be stored in Moodle's private directory. The experiment’s GUI and a live webcam stream are shown in Figure (17).



Current (mA) -1.31130218

Radiation sensor(W/m^2) -400.001311

Figure (17): A pilot renewable energy remote lab homepage.

Students can verify that the hardware platform reacts to the user interface controls and value changes by checking the live streaming of the webcam. At the end of each experiment, students verify that they typed all the code correctly before ending the session. Students give themselves enough time for the result to be downloaded by clicking the save button and saving it as an Excel file that can be downloaded. At the end of the task, students analyse the results and send them to the instructor through e-mail or Moodle.

5.4 Lab Chain: Securing Remote Lab Using Blockchain

The way Blockchain technology decentralises ledgers, creating a distributed database that is shared across a peer-to-peer network, is a paradigm shift. It allows for simultaneously decentralised yet intrinsically trusted transactions without a single point of failure or a single point of centralised control. This is possible because, in exchange for removing a trusted third party, the system relies on the distributed consensus that no single set of nodes can alter a Blockchain's contents without the network's explicit agreement. PoA consensus is an alternative to energy-intensive PoW systems. In PoA, a small set of validators are trusted by their reputation or validate transactions due to their pre-established position in the network. These validations are independently carried out, and then the validators go through an aggregating procedure across the nodes through the network that has been chosen as validators. PoA's speed comes from smart contracts running on the validators' hardware rather than wasting energy in every node. It means that PoA is especially suited to permissioned networks, where the nodes are not an unknown quantity because it offers benefits including speedier transaction processing, lower energy needs and better governance of the network, a prime model for consortium or private enterprise Blockchain networks needing to balance speed and throughput over absolute decentralisation (Rodrigues & Rocha., 2021) (Saini, et al., 2021) (Ncube & Terzoli., 2020) (Son, et al., 2021) (D & Maragatham., 2021) (Chan, et al., 2019).

An architecture called “Lab Chain” has been developed for managing remote laboratory data in a university environment using Ethereum private Blockchain as the ledger to store lab data from distributed sources using smart contracts. The flexible architecture presented in Figure (18) shows how web applications can interact with the Ethereum private Blockchain network to manage remote laboratory data in a university environment. Lab Chain's heart lies the Ethereum private Blockchain, upon which we built smart contracts to store this critical data.

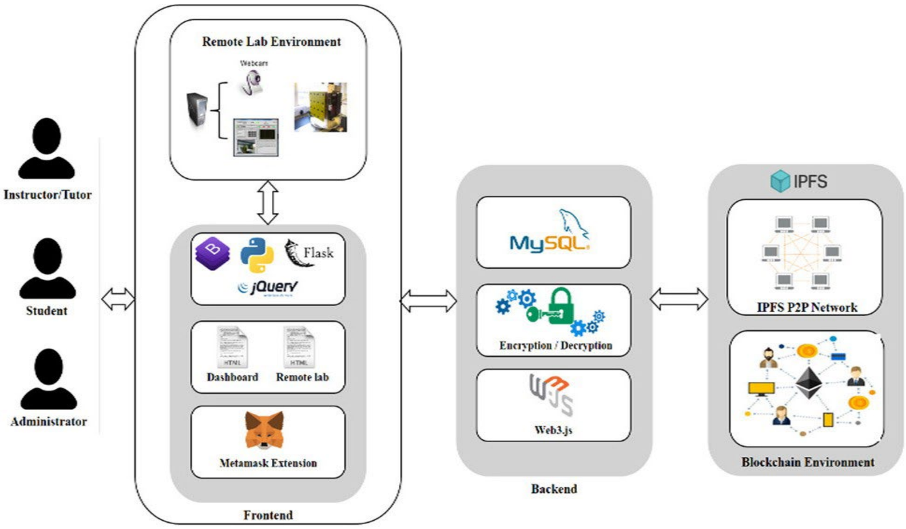


Figure (18): Proposed Blockchain-based remote lab management architecture.

Placing this data in a distributed ledger ensures data transparency, immutability, and decentralised control. Mapping (structure) and array (a multiple structure) used to create a data storage mechanism that is robust and scalable inside smart contracts for securing data. Another critical aspect we put in place was the IPFS for storing data. This started with a formalisation of the Lab Chain framework, setting up a symbiotic relationship between web applications and the Ethereum private Blockchain network, facilitating their interaction and data exchange: Each laboratory hosts its own Ethereum node that connects to the shared Blockchain in the network via the web3.js API and the Geth client. At a high level, the Geth client configures the nodes, enrols the nodes to the Ethereum network, and has access to the distributed ledger for transaction execution and data management. The features of decentralisation and tamperproof immutability of the records on the Ethereum private Blockchain ensure that remote laboratory data will be stored and can be made available to other authorised parties within the university community. The same features add to the trustworthiness and accountability of each consortium member. Moreover, a distributed architecture reduces the risk of sites or servers being singled out as attack points for malicious campaigns, making the system more resilient to failure.

Lab Chain addresses three related problems with remote laboratory data management in academia. It makes data more accessible to protect, more straightforward to verify, and easier to share and verify collectively, using open-source software that any research lab could set up. If the Blockchain technology utilized by LabChain can effectively guarantee the provenance of products, it may also be capable of ensuring the integrity and traceability of scientific experiments. This could enable more effective forms of individual and collaborative research than feasible today. It would help more labs do more science in new ways.

Implementing the Lab Chain protocol to manage remote laboratory data within a university setting follows a predefined data-flow process. Upon successfully deploying and setting up Lab Chain's private Ethereum Blockchain, the web app communicates with the Ethereum node using the HTTP protocol. To allow this communication, APIs (application programming interfaces) for Web3 are made available for commonly used programming languages such as JavaScript, Python, PHP, and others. The first step is to import the web3.js API, which defines the protocol to transfer the information stored on the Blockchain between the application on the browser and the Geth client. This web3.js HTTP request triggers the smart contract execution mechanism, which executes the pre-written rules and computations in the smart contract to manage the data securely and transparently from the remote laboratory.

One of the basic principles behind the development of Blockchain's is to interface every single instance of the management information systems and integrate it directly with the Blockchain infrastructure. Lab Chain is based on this architecture since it articulates a roadmap of how to link legacy Web 2.0 apps with Web 3.0 Blockchain’s through libraries and APIs that facilitate the connection with their nodes. Furthermore, the Lab Chain architecture described in the framework consists of a frontend, a backend and a service layer created by integrating the Ethereum platform with the IPFS. This architecture replaces existing learning management systems, such as Moodle, with a Blockchain-based architecture designed for organising and conducting remote laboratory sessions. The frontend layer of the Lab Chain comprises a CMS for students and instructors to interact with the remote lab environment. The backend layer handles the data on behalf of the users, carrying out the necessary processing and management using Ethereum Blockchain, IPFS and other decentralised solutions to store and retrieve controllable laboratory data under a distributed environment.

The Lab Chain framework allows the university to maintain its laboratory data remotely, using the Ethereum-private Blockchain's power and smart contracts. Figure (19) shows the flowchart of the design of the Blockchain learning management system. The development of the framework began by setting up our Ethereum Blockchain environment on a local and dedicated IPFS server. An Ethereum Node, web-server applications, and a MySQL database server are provisioned. Dashboard development: Programming in HTML, CSS, and JS, as well as a small quantity of Python, to interface with the HTTP method and communicate and interact with the Ethereum nodes. Learning management system development and deployment; Remix IDE for Solidity programme, a compiler used to create machine-level bytecode executed on the Ethereum nodes in the Ethereum VM, and smart contract testing, debugging and deployment. This is possible because all nodes in an Ethereum Blockchain are provisioned from Geth to enable decentralisation. The data produced by the experiment is distributed among all devices in the Blockchain: the third step is putting the students' data (theoretical or practically pulled from servers of the University Registration Authority) in an Excel spreadsheet.

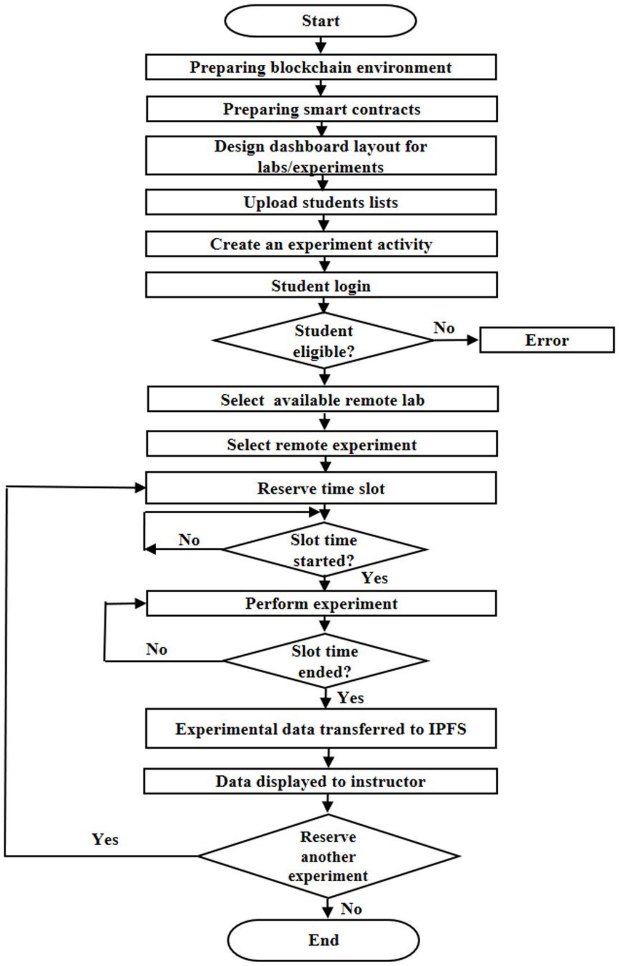

Start
Preparing blockchain environment
Preparing smart contracts
Design dashboard layout for labs/experiments
Upload students lists
Create an experiment activity
Student login
Student eligible?
No
Error
Select available remote lab
Select remote experiment
Reserve time slot
No
Slot time started?
Yes
Perform experiment
No
Slot time ended?
Yes
Experimental data transferred to IPFS
Data displayed to instructor
Yes
Reserve another experiment
No
End

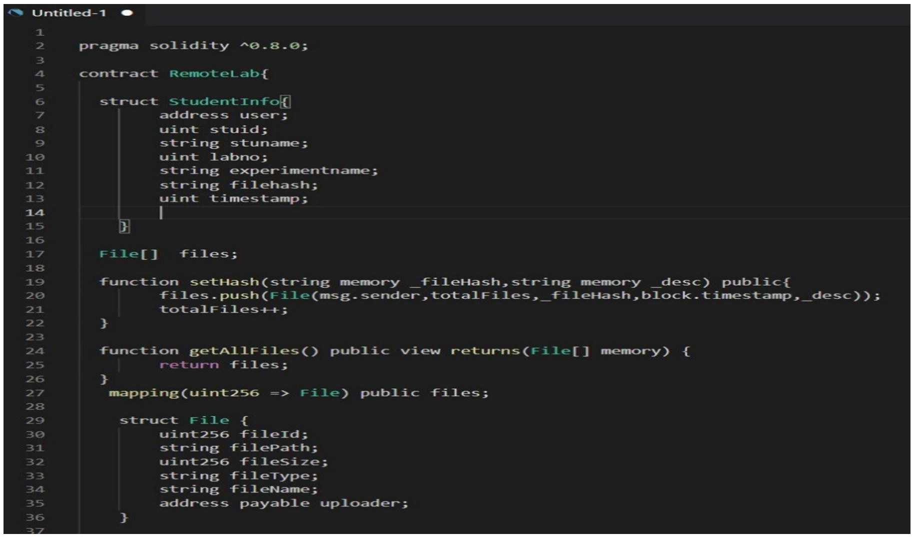
Figure (19): Flowchart of design of the Blockchain learning management system.

The registrar lists students, including their name, number, and specialisation. This list of students is then entered into a MySQL database server on which an admin can keep a record. Geth is also creating trial accounts. A Geth creates accounts by generating two hash keys (public and private key) – a public key as the student's anonymous ID and a private key as a password that the system will accept. Students are granted some Ether (the currency of Ethereum) that they can spend to connect to a remote lab (coded inside a browser's extension called MetaMask) over an off-chain data management system ("Registered student" status is true if the connected account is a student from the enrolled student list and false otherwise).

The list of labs and corresponding experiments in remote labs will be displayed on the dashboard, and the experiment name, duration, URL, and data web service link will be included. After a student submits the private key to the smart contract's user dashboard home page, they can search for remote experiments available, book sessions within an allotted time window, and then run the experiments using the instructions provided. Once the experiment is triggered, the trial has been tracked, and the confirmation payment has been captured. Then, the SOLIDITY Mapping Array will download the experiment data (streaming from the experiment) until the allocated time expires. From the SOLIDITY Mapping Array, the experiment data (streaming from the experiment) are transmitted to the IPFS location for the smart contract in the form of Excel sheets to allow the record of experiment data for archive purposes. Suppose a lecturer or teacher asks for the evaluation of a paper by a particular student. In that case, the lecturer's or teacher's details are extracted from the MySQL server. The relevant experimental data is simultaneously extracted from the Blockchain mapping array and IPFS and evaluated. By using Ethereum private Blockchain, smart contracts and IPFS, Lab Chain provides a secure, transparent, and decentralised environment for remote laboratory data management, enhancing collaboration and increasing the efficiency of scientific research across the university community.

5.5 Secure and Transparent Learning

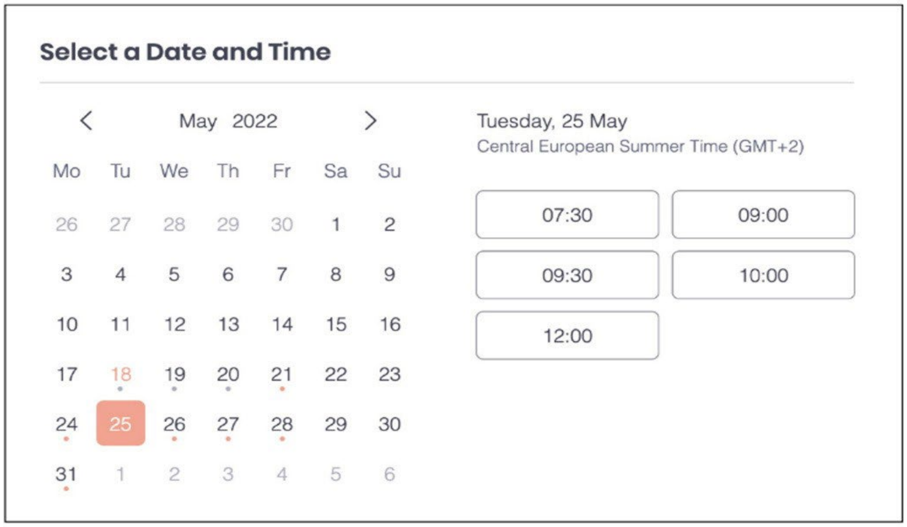
The remote data management system was first tested on a renewable energy lab consisting of rooftop solar panels and wind turbines. These experiments were programmed in a graphical language named LabVIEW, which was installed on the web server. The obtained data was transferred to the lab computers via a programmable automation controller. Wind and Photovoltaic Energy illustrates a laboratory to nurture students' knowledge of the properties of PV panels and wind generators. Students will develop their skills by monitoring PV panels and wind turbines' output current, voltage, and power. Other experiments include measuring the voltage, wind speed, battery voltage and load current. In this laboratory, students can study the photovoltaic panels, temperature, wind speed, battery voltage, load current experiments and measurements. Another experiment was to set up load boxes and parameters and measure IV of PV modules. This also assists in measuring the current by varying the angle of incidence and distance. Figure (20) shows how a smart contract is written to create student records on the Blockchain. The structure 'StudentInfo' is defined as the most key details to be stored. The name of the student, ID, Lab no., Name of the experiment, hash of the student's uploaded streaming data given by IPFS, and time stamp in the block while the blocks are added in the Blockchain to record the approximate time the student has uploaded the streaming data file. The smart contract consists of two vital functions. The first is setHash, which passes the principal parameter as a hash string of the student-uploaded streaming data file. It is a public function that can be called from an external contract. The second is experiment Info, calling once a new recording is created. Since a function can only send a transaction to the Blockchain, the output is not visible until it is mined and added to the Blockchain. Every transaction made on the Ethereum platform requires a fee paid in ether as it incurs a mining cost to confirm and add the block in the Blockchain. This task was carried out using MetaMask. MetaMask is a cryptocurrency wallet that can be used as an extension of Chrome and Firefox browsers.



```

pragma solidity ^0.8.0;

contract RemoteLab{

  struct StudentInfo{
        address user;
        uint stuid;
        string stuname;
        uint labno;
        string experimentname;
        string filehash;
        uint timestamp;

    }

  File[]  files;

  function setHash(string memory _fileHash,string memory _desc) public{
        files.push(File(msg.sender,totalFiles,_fileHash,block.timestamp,_desc));
        totalFiles++;
  }

  function getAllFiles() public view returns(File[] memory) {
        return files;
  }
   mapping(uint256 => File) public files;

    struct File {
        uint256 fileId;
        string filePath;
        uint256 fileSize;
        string fileType;
        string fileName;
        address payable uploader;
    }
```

Figure (20): Source code of the implemented smart contract.

A task-specific smart contract has been designed to accept requests for booking sessions. The smart contract structure is depicted in the screenshot of Figure (21), which shows how the students remotely reserve the time slot by clicking on the "book" button on the right-hand side of the calendar. The student and the system administrator can edit or delete the session.



Select a Date and Time

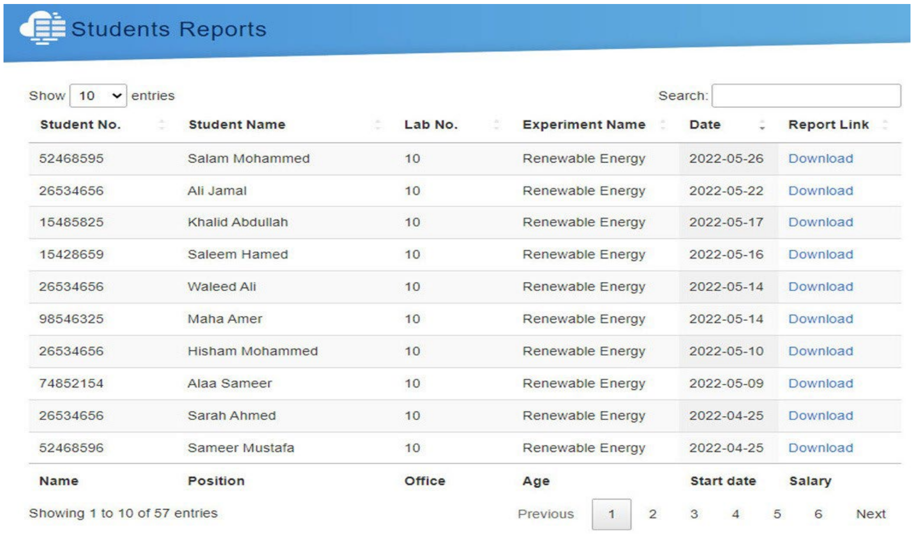
< May 2022 >

Mo	Tu	We	Th	Fr	Sa	Su
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Tuesday, 25 May
Central European Summer Time (GMT+2)

Figure (21): Students' scheduling scheme.

When students have experimented, they can download their reports from the Blockchain and the IPFS and list them on a particular page, like in the Figure (22) screenshot. It should contain a student's university number and name, the lab number and title of the experiment, its date, and the report. Now, the instructor can see and download all submitted reports, student information, and files containing the experiment results for grading.



Students Reports

Show 10 entries Search:

Student No.	Student Name	Lab No.	Experiment Name	Date	Report Link
52468595	Salam Mohammed	10	Renewable Energy	2022-05-26	Download
26534656	Ali Jamal	10	Renewable Energy	2022-05-22	Download
15485825	Khalid Abdullah	10	Renewable Energy	2022-05-17	Download
15428659	Saleem Hamed	10	Renewable Energy	2022-05-16	Download
26534656	Waleed Ali	10	Renewable Energy	2022-05-14	Download
98546325	Maha Amer	10	Renewable Energy	2022-05-14	Download
26534656	Hisham Mohammed	10	Renewable Energy	2022-05-10	Download
74852154	Alaa Sameer	10	Renewable Energy	2022-05-09	Download
26534656	Sarah Ahmed	10	Renewable Energy	2022-04-25	Download
52468596	Sameer Mustafa	10	Renewable Energy	2022-04-25	Download
Name	Position	Office	Age	Start date	Salary

Showing 1 to 10 of 57 entries

Figure (22): Blockchain page for retrieved students' experimental reports.

By embracing a 'distributed' learning ecosystem, Blockchain was selected by many users as the LMS of choice. Since a Blockchain is a 'distribution' of the ledger across its nodes, it is unmatched in resilience to hacks and vulnerabilities. A Blockchain in a fully distributed network removes the ‘failure point’ from a single central point of vulnerability. If one node fails – all the data is not in the exact single location – then the robust programming where most networks are set up so that all the nodes have a full copy of the data means nothing can be lost.

This is vastly different from the single point of failure for Moodle and all other open-source applications stored on a centralised server like the one with Moodle. Besides, because private and public keys fully encrypt all the data, the distributed Blockchain-based database is far safer than any private enterprise venture with which Moodle is affiliated. Moodle is not designed to run large amounts of data involving transactional events with which users can now squeeze far more usable and assignable information to students without losing privacy and transparency. However, when a decentralised Ethereum Blockchain is built, it allows transactions and contracts to be built without having ether in them; thus, it cuts down the transactional costs.

5.6 Chapter Summary

Blockchain technology is pivotal in ensuring the secure management of data generated across diverse ecosystems at any time and place. This chapter presents an innovative Learning Management System (LMS) based on Ethereum, designed explicitly for remote laboratories. This system facilitates streaming data transmission to a decentralised infrastructure, thereby showcasing Blockchain's potential in handling substantial datasets produced by remote labs. The approach guarantees an unbiased, secure, and transparent management process while safeguarding the confidentiality of student files and reports.

The Lab Chain initiative is emerging as a transformative solution for managing online experiments, indicating a significant shift away from traditional lab lectures. This advancement heralds the onset of "labs 4.0," which promises to broaden the scope of engineering education. Integrating Massive Open Online Courses (MOOCs) and other educational innovations—such as augmented reality, big data analytics, 3D printing, and machine learning—will effectively supplant conventional teaching methodologies. This evolution signifies the dawn of Education 4.0, where decentralised, transparent, trustworthy, and secure access to lectures and laboratory experiments will become standard practice in lifelong learning initiatives.

The development of a Blockchain-based LMS enhances the educational experience and establishes a robust framework for future educational paradigms. By leveraging Blockchain technology, this system provides a reliable mechanism for managing educational resources and student interactions in a way that promotes integrity and accountability. The results indicate that such systems can significantly improve the accessibility and quality of education, setting a new benchmark for how remote learning environments are structured and operated.

In the next chapter 6: Machine Learning-Driven Real-Time Prioritization, in the chapter a machine learning-driven real-time priority system for vital signs of ICU patients in the Blockchain network is introduced. The Data Prioritizing algorithm, its steps, normalisation, and implementation are shown. This chapter demonstrates the ability to integrate machine learning to promote the value and performance of the proposed solution.

Chapter 6

Machine Learning-Driven Real-Time Prioritization of ICU Patient Vital Signs in Blockchain Networks

The rapid development of the IoT and Blockchain technologies and their fast adoption in various application areas have pushed the world toward integrating smart devices. The fusion of BCoT will improve operational efficiency, data security, and innovation by enabling business and social processes to trust, coordinate and collaborate without a central authority. Data will be generated by the devices and processed, exchanged, and used by the BCoT systems. This big data is so massive that new and more powerful prioritisation methods and organisations must be developed. Managing big data from BCoT systems effectively so that it can be put to optimal use is a necessity. Here, a novel architecture is proposed for securing data and managing them using the prioritisation procedure with PMML by first taking a static dataset with human vital signs from the University of Queensland to derive their baseline ranges and, after that, calculating dynamic weights using trends in the patient's data and those ranges for each parameter. All the data above these calculated thresholds will be marked as a high priority. This will allow immediate dispatch of alerts and appropriate action that can be triggered for the patient. The validity of the approach was demonstrated by using PMML for the Random Forest classifier in predicting alarm conditions, with an impressive average accuracy of 99.53%. This high accuracy shows that the algorithm targeted for joining health data learns more complex patterns and dependencies than other methods. This might provide higher accuracy for classifying alarm conditions, improving patient outcomes.

6.1 Introduction

The fast evolution of the IoT means that it is being applied in ever more industry sectors. Healthcare is one of the most important. It is essential that the IoT devices being used can be trusted to produce secure data. The BCoT guarantees the security and provenance of data in an Internet of Things by making tamper-resistant records of all shared transactions, thereby providing greater transparency, preventing fraud, and maximising the efficacy and cost-efficiency of operations (Yadav & Vishwakarma, 2022) (Zhang, et al., 2020). Specific challenges in Blockchain technology need to be overcome. The architecture and operational aspects of the BCoT allow us to integrate and use AI engines in the devices to produce better outcomes that address data issues such as scalability, timeliness, heterogeneity, inconsistency, confidentiality, and, however, the distributed nature of IoT devices and edge nodes are under the threat of malicious operation. Data security is often seen as a significant concern due to the interception and tampering of data during transmission and storage. Other issues with BCoT include weak authentication mechanisms, insufficient access control policies, etc. Various architectures and frameworks have been proposed to address these challenges for secure data storage and management in BCoT networks (Abadi, et al., 2018) (Zhang, et al., 2020) (Sadawi, et al., 2020) (Liu, et al., 2021) (Al-Nbhany, et al., 2024).

Prioritisation of the big data submission is another major issue in BCoT applications, such as healthcare, where specific data from a patient in an intensive care unit must be given priority over others. Van Rossum et al. suggested evaluating the alarm strategies for continuously monitoring vital signs in patients on a post-surgical ward. The classical fixed-threshold alarming strategy was compared against six simulated adaptive strategies, which changed the alarm thresholds based on personal or patient factors. Although the classical approach detected some adverse events, some specific adaptive strategies were more sensitive in detecting events or lowered the overall alarm numbers. A combination of multiple adaptive strategies worked best, allowing the early detection of adverse events while keeping the alarm rates as low as possible. However, this study has inherent limitations, such as being a small retrospective study, and more research is required to confirm the clinical benefits of the adaptive alarm strategy (Rossum, et al., 2022).

An intelligent architecture that integrates edge-computing, AI, IoT, and Blockchain technology in healthcare, particularly for real-time prioritisation of patient vital sign data in intensive care units (ICUs), is presented in this chapter. In the IoT and edge computing paradigm, the RPi4 device can empower an IoT edge node, which means that the RPi4 will collect, aggregate, and analyse IoT data from sensors and actuators on the edge of a network. This architecture functions as both a data architecture and a software architecture for AI and Blockchain technologies. It will move the intelligent point to where the information extraction from the data occurs. Another crucial pillar of this system is a Random Forest AI classification engine deployed on RPi4 devices, utilising PMML for on-premises execution. The intelligence will move toward the edge in a way that accelerates the data-processing cycle, ultimately allowing the system to operate more efficiently. These RPi4 devices receive IoT sensor data from an ICU environment once data is captured, streamed, and continuously monitored and collected in real-time. In this context, the Random Forest model was trained on the University of Queensland vital signs dataset to classify surgical outcomes or identify patterns related to anaesthesia monitoring (Liu, et al., 2012).

The Blockchain infrastructure is built into a private Blockchain to store and distribute processed data from the edge devices and AI-driven insights from the classification engine. Blockchain technology acts as a system, infrastructure, and service to provide organisation and 'trust' associated with the data. The system assumes tamper-proof data integrity over its lifetime, accomplished by end-to-end encryption.

This novel BCoT architecture composed of sensors, AI, edge computing and Blockchain components are tested according to specific conditions and standards to verify the correctness of the BCoT architecture-based decision-making and the behaviour of the components that compose the architecture of the BCoT under stress until a final decision is made. This way, the system can take advantage of every component at its best, making decisions in real-time in a safe, fast, and intelligent manner and being able to process, analyse and generate data. This feature is particularly useful for high-criticality applications in healthcare.

6.2 Proposed BCoT Architecture

As shown in Figure (23), the BCoT architecture provides a cost-effective scheme for effectively obtaining, processing, analysing, and disseminating securely any data that comes into emergency room environments in real-time. This is done using Blockchain technology in three pivotal layers: the first intended for data acquisition, the second for data processing, and the last for data analysis, dissemination, and access control. These layers will be described further in subsequent sections.

1. The sensors layer is the first one in an IoT architecture. It can be seen as an essential layer of devices, such as sensors, devices, and actuators. It can sense and perceive the physical world, such as the IoT sensors deployed in a patient room to sense vital signs, patient conditions, and the physical environment. Sensors in this application act as sentinels, sitting on the frontline of care and capturing live data. The output of these sensors is then transmitted to the other level of IoT architecture.
2. Network Layer: The second layer assumes that the data collected from the sensors is sent to the RPi4 devices (or other processing units), ensuring that this job is done reliably and efficiently. At this Layer, data transmission aims to maintain the integrity of the information, keeping it safe from loss or corruption at any point on its path towards a processing stage.
3. Processing Layer: The final processing layer encompasses the transformation journey of raw data into actionable information. This conceptual layer benefits the most from various edge technologies for analysing and synthesising raw data. The robust edge nodes with rigged computational AI/ML equipment, such as those powered by the RPi4, are technically the vital processing machines in this context. Using advanced algorithms and predictive models, raw data is fed into the edge node, where the edge node processes, analyses, and synthesises the raw data to provide information in this critical phase. The adaptive thresholds help the system to fine-tune the threshold readings based on the criticality of data. This helps the system to process the high-priority information faster than other low-priority information immediately, so it does not miss out on the red flags and interventions when most needed by identifying anomalies early on.

Within the Processing Layer, a crucial sub-component, termed 'Secure Outcome Sharing', exists for disseminating analytical results. This element serves as the terminus of the analytical pipeline, where the outputs from various predictive and analytical systems are encoded and distributed across a decentralised network infrastructure. The transmission of these findings leverages Blockchain technology, specifically an internal Ethereum-based network, which provides a secure conduit for data propagation. This approach ensures that the shared outcomes possess inherent qualities of immutability, transparency, and resistance to tampering. The 'Secure Outcome Sharing' mechanism facilitates the distribution of insights and recommendations to authorised stakeholders within the Ethereum Blockchain architecture. This arrangement grants these entities unrestricted and immediate access to critical information, enhancing their analytical capabilities and decision-making processes.

This architecture leverages distributed ledger technology to create a strong framework for information dissemination, distinguished by its resilience, traceability, and capability for real-time data access. It enhances the integrity of shared results and fosters a more efficient and transparent analytical environment for all participating entities.

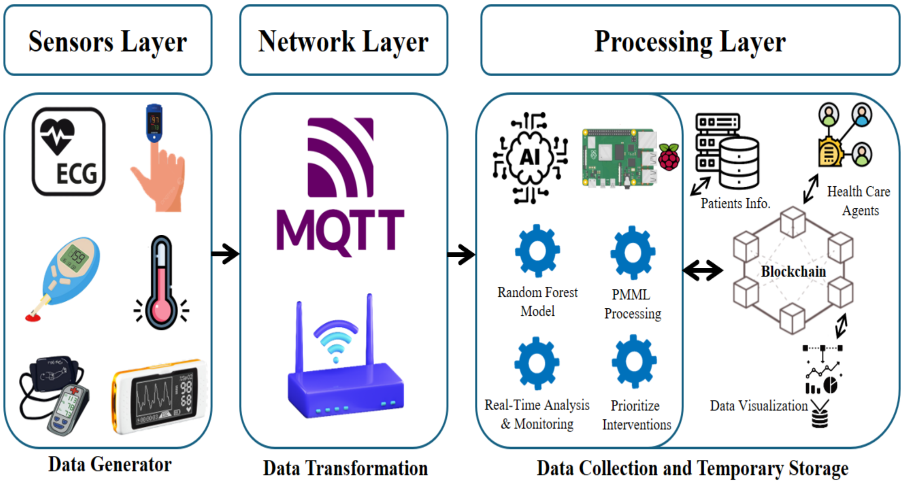


Figure (23): Design of the proposed experimental system.

This multi-layered architecture is enabled by the hardware components in place, where the IoT sensors embedded in patient rooms collect data in real-time and communicate it via secure transmission protocols like MQTT to edge nodes and RPi4 devices. The inferences are performed on-device using the AI classification model exported as a PMML file (for example, if the data collected arrived at the sensor and confirmed that the patient had an irregular heartbeat, then it is inferred that their risk of a heart attack is predicted on the edge device using the AI model and is displayed on display); the edge nodes are also capable of being equipped with computational power and their AI to perform inferences on the data in real-time to alert the healthcare agents. In addition, Blockchain is utilised to develop a complex distributed network of nodes that validate the transactions and append the following block to the distributed ledger, persisting data while ensuring the integrity of the information. Therefore, in this use case, a secure, intelligent, and decentralised data management system is implemented in the emergency rooms using IoT sensors, edge computing, AI models and Blockchain technologies. This multi-layered architecture and careful selection of dedicated devices provide real-time, low-latency responses that can spoil patient outcomes in each millisecond.

6.2.1 Vital Signs Dataset Preparation

The high-resolution, time-synchronised vital signs collected from multiple anaesthesia equipment cover the whole surgical procedure; this dataset was developed to overcome the limitations of traditional AIMS in collecting good-quality vital signs data for research purposes. The vitals captured include bio-signals commonly monitored in the operating room – such as blood pressure, heart rate, oxygen saturation and respiratory rate. The data were extracted from 32 surgical patients using free software called the Vital Recorder program developed by research team at the University of Queensland that automatically collects and synchronises bio-signals from several medical devices.

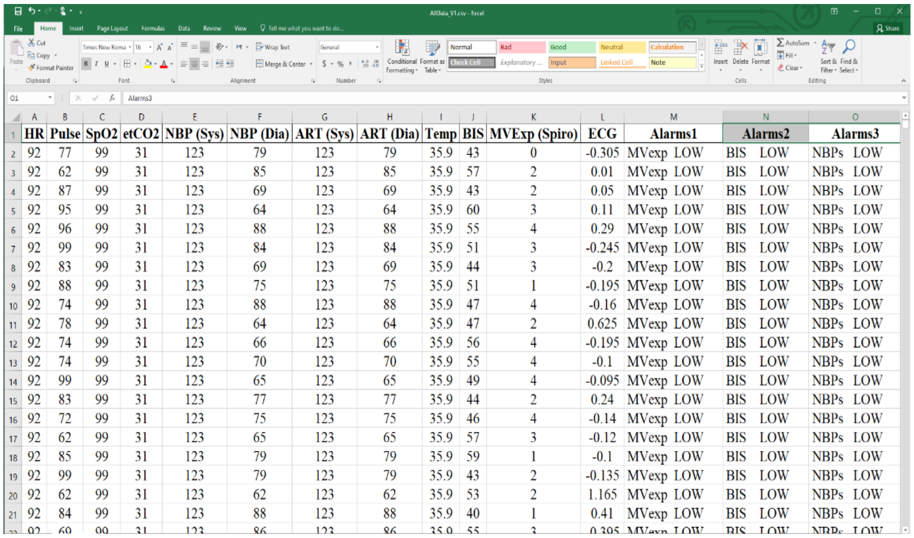
Creating the dataset was motivated by the limited availability of good-quality, multi-parameter bio-signals data for research in patient monitoring, early identification of clinical deterioration and early warning scores, and development of predictive models for adverse events. This dataset also includes interventions such as medication infusions and ventilation that may be linked to adverse events. The high-resolution, time-synchronised, multi-parameter bio-signals data collected from multiple anaesthesia equipment cover the whole surgical procedure. They are valuable precursors to developing physiologically based scoring systems that detect interactions between elements of complex interventions. These datasets serve the long-term vision of finding more sophisticated approaches to prevent adverse events, improve patient safety during surgical procedures and enhance clinical decision-support systems. The dataset is freely available to researchers worldwide through digitised data resources and archives such as PhysioNet, which has contributed significantly to medical advances for many decades (Liu, et al., 2012).

This dataset was used to test the proposed system with a subset of 12 parameters. As in the training dataset, more than one file with readings was available, so these files and their rows with empty cells or null values would have to be dealt with. So, initially, in each file, rows with empty or null values were removed once by iteration. However, an advanced way of removing missing values is to apply an imputation method with the best accuracy for that dataset. Therefore, a more advanced technique, KNN, is used to find missing values. KNN imputation looks at the similarity between instances using the K-nearest neighbours' algorithm and imputes values based on more recognisable patterns and relationships in the data. Hence, both techniques (filling blanks and imputation) form a dual process, where the dataset is cleansed of incomplete rows and filled with imputed values, making it ready for the proposed system.

In Addition, this dataset was analysed, and the most critical parameters for the system testing were identified. The twelve parameters are most relevant for the testing scenario, which are Heart Rate (HR), Pulse Rate (Pulse), Blood Oxygen Saturation (SpO2), End-Tidal Carbon Dioxide (etCO2), Non-Invasive Blood Pressure (Systolic) (NBP (Sys)), Non-Invasive Blood Pressure (Diastolic) (NBP (Dia)), and Arterial Blood Pressure (Systolic) (ART (Sys)), and Arterial Blood Pressure (Diastolic) (ART (Dia)). Other vital signs data, such as temperature (Temp), Bispectral Index (BIS), Minute Volume Expiration (Spirometry) (MVExp), and Electrocardiogram (ECG), would probably be necessary.

As soon as these parameters were identified, as shown in Figure (24), a new flattened dataset was created with only those columns, which was done by iteration once in each file. Regarding dealing with alarm columns, if they were present in the dataset, their values probably depended on some readings from other parameters; so, a set of rules or thresholds based on the selected vital signs was determined.

An example is that if the heart rate was over a specific value, or if the blood pressure was below a specific value, the alarms column can be set to an alarm condition, or if the dataset already contains alarm columns, they were included in the new dataset in this form and were used for testing and evaluation.



HR	Pulse	SpO2	etCO2	NBP (Sys)	NBP (Dia)	ART (Sys)	ART (Dia)	Temp	BIS	MVExp (Spiro)	ECG	Alarms1	Alarms2	Alarms3
92	77	99	31	123	79	123	79	35.9	43	0	-0.305	MVexp LOW	BIS LOW	NBPs LOW
92	62	99	31	123	85	123	85	35.9	57	2	0.01	MVexp LOW	BIS LOW	NBPs LOW
92	87	99	31	123	69	123	69	35.9	43	2	0.05	MVexp LOW	BIS LOW	NBPs LOW
92	95	99	31	123	64	123	64	35.9	60	3	0.11	MVexp LOW	BIS LOW	NBPs LOW
92	96	99	31	123	88	123	88	35.9	55	4	0.29	MVexp LOW	BIS LOW	NBPs LOW
92	99	99	31	123	84	123	84	35.9	51	3	-0.245	MVexp LOW	BIS LOW	NBPs LOW
92	83	99	31	123	69	123	69	35.9	44	3	-0.2	MVexp LOW	BIS LOW	NBPs LOW
92	88	99	31	123	75	123	75	35.9	51	1	-0.195	MVexp LOW	BIS LOW	NBPs LOW
92	74	99	31	123	88	123	88	35.9	47	4	-0.16	MVexp LOW	BIS LOW	NBPs LOW
92	78	99	31	123	64	123	64	35.9	47	2	0.625	MVexp LOW	BIS LOW	NBPs LOW
92	74	99	31	123	66	123	66	35.9	56	4	-0.195	MVexp LOW	BIS LOW	NBPs LOW
92	74	99	31	123	70	123	70	35.9	55	4	-0.1	MVexp LOW	BIS LOW	NBPs LOW
92	99	99	31	123	65	123	65	35.9	49	4	-0.095	MVexp LOW	BIS LOW	NBPs LOW
92	83	99	31	123	77	123	77	35.9	44	2	0.24	MVexp LOW	BIS LOW	NBPs LOW
92	72	99	31	123	75	123	75	35.9	46	4	-0.14	MVexp LOW	BIS LOW	NBPs LOW
92	62	99	31	123	65	123	65	35.9	57	3	-0.12	MVexp LOW	BIS LOW	NBPs LOW
92	85	99	31	123	79	123	79	35.9	59	1	-0.1	MVexp LOW	BIS LOW	NBPs LOW
92	99	99	31	123	79	123	79	35.9	43	2	-0.135	MVexp LOW	BIS LOW	NBPs LOW
92	62	99	31	123	62	123	62	35.9	53	2	1.165	MVexp LOW	BIS LOW	NBPs LOW
92	84	99	31	123	88	123	88	35.9	40	1	0.41	MVexp LOW	BIS LOW	NBPs LOW
92	69	99	31	123	86	123	86	35.9	55	3	0.395	MVexp LOW	BIS LOW	NBPs LOW

Figure (24): Screenshot of the normalised dataset of Queensland University.

6.2.2 Machine Learning Algorithms

Machine learning algorithms are a subset of AI that allows learning and improving from experience for algorithms that are not explicitly programmed for a task but instead 'learn' by being exposed to data without requiring domain expertise (Sinclair, et al., 1999). These types of algorithms allow the machine to find patterns in data. Some standard machine learning algorithms are supervised, unsupervised and reinforcement learning. Supervised learning algorithms train machines from input data with an associated output value. This association between input and output values is a training set in machine learning. Each involved entry is referred to as a data record composed of one or several input fields and a single desired number (in case of regression problems) or class (in case of classification problems). For example, in an input that provides a single patient's medical record, each data record could describe an individual's medical history, with the desired number being the person's survival time after surgery. Another type of algorithm is called an unsupervised (self-organising or self-teaching) learning algorithm, which is an automated process of finding patterns and relationships in the data without any labelled input (unlabelled data). The algorithm carries out this process of identifying the underlying factors without any human intervention or a specific purpose for the data. A simple but popular algorithm available under this category is called clustering. K-means and hierarchical clustering are examples of unsupervised algorithms. Reinforcement learning algorithms are used when the learning agent must interact with its environment to find an optimal solution to maximise its performance based on its objective. The agent assesses its performance by acting, observing the consequences, and receiving feedback or a reward/penalty. This feedback is used to learn about the best action in a specific context. Examples of the applications of reinforcement learning algorithms include game-playing, robotics, and other related decision-making tasks. These include self-driving cars, industrial robots, and other toys. In each application, the agent aims to maximise its performance or reward relative to its goal. A solar-powered thermostat is one such way of using reinforcement learning. Some applications of machine learning algorithms are automated text and sentiment categorisation, intrusion detection for computer networks, filtering junk e-mail, credit card fraud detection, detecting patterns of customers' buy behaviour, optimising a manufacturing process, and modelling the spread of diseases. The most significant number of applications (except game playing) involve supervised versions of machine learning algorithms rather than unsupervised ones (Sinclair, et al., 1999) (M, et al., 1998) (Aleskerov, et al., 1997) (Kim, et al., 2003)

A random forest algorithm was used (ensemble learning is a powerful machine-learning technique that combines many individual learning algorithms to obtain better predictive performance and reduce variance or overfitting to noise in the training data). A random forest combines the wisdom of crowds by 'averaging' the predictions of many individuals' 'decision' (or 'classification and regression') trees. A key idea in a random forest is that many decision trees are constructed. Each tree is built on a different random sub-sample of the training data (using a bootstrap sampling idea) — that is, some records in the training sample will be sampled more than others. Also, a different random subset of features is considered for a split at each node within the tree-growing process (Scornet, et al., 2014). The input data is run through the trees in the forest to predict the new case. Each tree votes for the predicted class (in classification problems) or scores the case in terms of a real-valued attribute (in regression problems). The final prediction is obtained by taking most of all tree votes for classification or the mean of all individuals' scores for regression. Because the individual trees are not guaranteed to agree on the prediction, this ensemble approach captures the different trees' knowledge, cancelling the impact of individual trees' dependence or bias and reducing their potential variability by taking the average. The random forest algorithm is well suited for capturing complex patterns, can easily handle high-dimensional data and is very robust when most of what one wants to predict cannot be explained by the data (e.g. in weather predictions where objects cannot be separated into 'rain' and 'no rain'). Because there can be more trees than data (hundreds, thousands, sometimes hundreds of thousands), the average of the votes has a spurious regularising effect (so that when there is noise or an outlier in the data, it will have minor impact on predicting the new case). Moreover, the random forest is easy to use and implement and has been applied to the broadest range of problems, from image recognition to bioinformatics and financial modelling. Figure (25) below depicts the random forest algorithm (Sarica, et al., 2017).

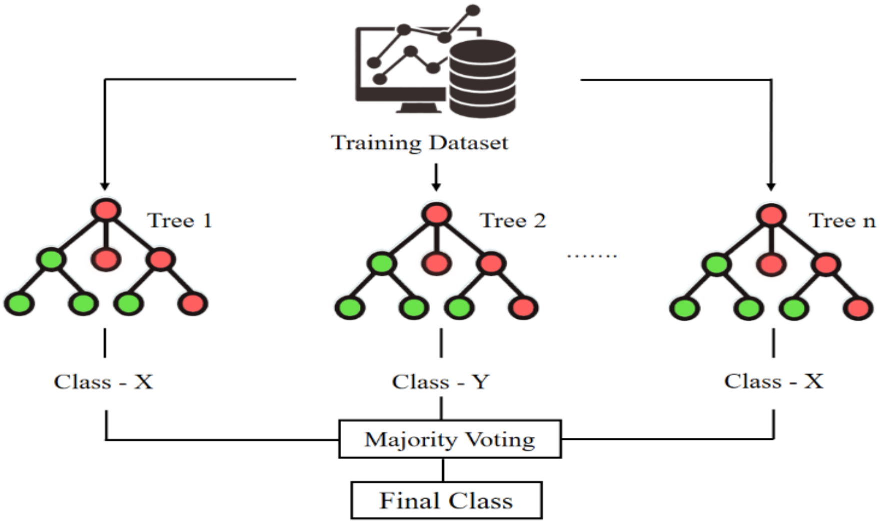


Figure (25): Random Forest architecture.

The flowchart in Figure (26) illustrates the process of training and validating Random Forest Classifiers on a medical dataset stored in Google Drive. The process begins by importing required libraries or packages for data manipulation, machine learning and PMML conversions like pandas, sci-kit-learn, and sklearn2pmml. The next step is to connect to the CSV files saved to Google Drive. This step also involves loading the dataset and pre-processing the dataset by replacing NaN values with 'N/A' and then shuffling the data at random. Moreover, the dataset's features (X) and target variables (y1, y2, and y3) are separated, and data is split into training and testing sets for each target variable. In the next step, the Random Forest Classifier initialises as a classifier by taking in different hyper-parameters and trains the classifier on training data and target variables.

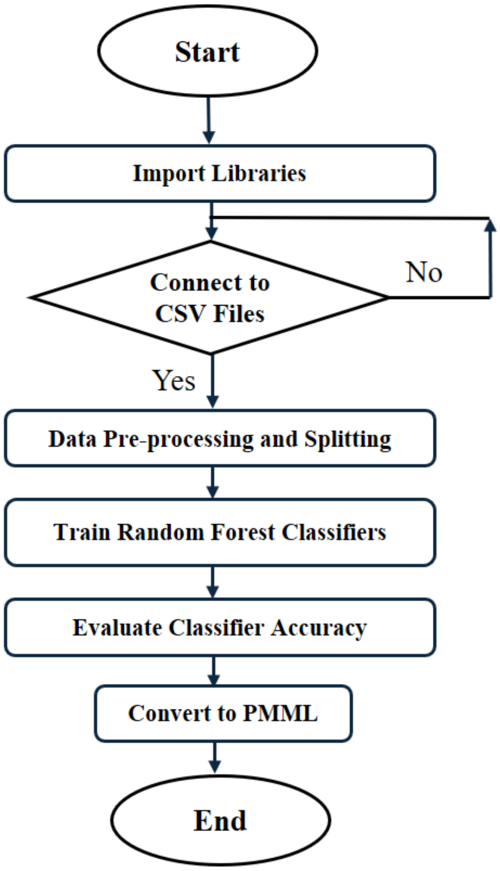

Start
Import Libraries
Connect to CSV Files
No
Yes
Data Pre-processing and Splitting
Train Random Forest Classifiers
Evaluate Classifier Accuracy
Convert to PMML
End

Figure (26): Flowchart of the training and evaluating random forest classifier.

The trained classifier predicts the test data, measures accuracy per target variable and prints classifier accuracy. To train and evaluate the Random Forest Classifier on patients' normalised sensor data, predict three alarm conditions based on the sensor data, save trained models to Google Drive, and export the trained models in PMML format. In each step, the algorithm trains the model and checks if all the alarms are detected when evaluating the model. The code sets patient data in the Data Frame and takes 20% of the file for testing, which leaves 80% for training the algorithm. Therefore, the script trains two classifiers (2-fold algorithm) – one which executes tests for 80% of the data and infers 20% of it, and another that inversely tests and infers. When checking two algorithms, the evaluating algorithm minimises the confusion matrix, the critical quality metric. In the case of the Confusion Matrix, if true/positive and false/positive errors are equal (0.45), while false/negative or accurate/harmful errors are relatively lower (0.2), it means the algorithm is doing a great job in detecting instances of the classes and incurring only half as many false positives (predictions). After evaluating the classifier, the code makes trained models portable and interoperable by converting them to PMML, a portable and interoperable standard, and saving them to the directory specified in Google Drive. This step is essential for deploying machine-learning models for AI systems, such as the mechanism described in the proposed system architecture. The trained models were exported as PMML files and would be helpful for model deployment and AI system integration.

The normalised vital signs data set offers an opportunity to develop predictive techniques of alarm conditions based on the data taken during a surgical procedure using state-of-the-art machine learning approaches. This study utilised the Random Forest algorithm as a classifier model for predicting the three-alarm columns present in the dataset. Random Forest is an ensemble method of learning based on multiple decision trees introduced to address the issue of variance reduction. It combines a set of decision trees into a single predictive model. Hence, it is considered an averaging method over separate decision trees, with each tree possessing weak learning capabilities except for combining different trees contributing to high predictive accuracy. Random Forest is suitable for the current study because of its ability to handle large-dimensional data, along with its ability to capture complex, non-linear relationships between input features and target variables. This is particularly beneficial when vital signs parameters are represented using high-dimensional features. In contrast, an alarm condition falling under a particular threshold of vital signs parameters can be achieved by combining subtle differences between different patients (the variations in vital signs parameters) and normalising (aligning) them to the predictive boundary between a class of medical patients. The dataset has three alarm columns, each representing a different kind of alarm condition corresponding to particular combinations or thresholds for the vital sign's parameters.

The objective was to create a predictive model to accurately classify the occurrence of these alarm conditions using the vital signs data recorded during attendance. The data should be split between training and testing sets to facilitate model development and evaluation. The training set was used to train the machine learning models. The testing set was reserved to evaluate the performance of the trained models. When splitting the data for training and testing, care was taken to ensure that if an alarm occurred in the sample, the distribution of alarm and non-alarm conditions was maintained so that the trained model's ability to detect alarms would be fairly evaluated. Stratified sampling techniques were typically required, mainly if the alarm did not often occur compared with non-alarm conditions. Machine learning is excellent for identifying subtle patterns and relationships. Training and evaluating the Random Forest model on this dataset resulted in reporting an overall impressive average accuracy dependent on the patient data, 99.5% for alarm conditions. This accuracy indicates that the Random Forest algorithm captured how the patient's vital signs contributed to alarm conditions with little error. These features 'voted' on an event as alarm or non-alarm, usually finding consensus and, therefore, more likely to capture the underlying dynamics when vital sign data is disordered. Since Random Forest comprises an ensemble of decision trees, the risk of overfitting the data and producing a model that provides an optimistic assessment of the model's ability to generalise to unseen data is mitigated.

6.2.3 Enhancing Medical Alarm Accuracy and Efficiency with Machine Learning

High accuracy is essential to develop a mechanism that can produce signals about probable sickness based on medical alert systems (Clifton, et al., 2013). Applying machine learning algorithms to predict an alarm condition based on the medical sensor data parameters can help doctors monitor patients. From the current industry research perspective, machine learning can do miracles in predicting alarm conditions by directly applying random forests to medical data. Applying Random Forest classifiers yields promising results in predicting three distinct alarm conditions. The prediction accuracy demonstrates strong similarity in forecasting parameters that exceed their limits. The highest accuracy found is nearly 98.81 % for one of the alarm conditions where the parameter specified in the record is considered outside of the normal range. They can make a model that is close to the original system since it fits training data well and generalises to unseen data. This shows that the random forest classifier can predict the medical parameter based on training data. So, random forests can be helpful in early warning systems to save human lives by predicting future events based on medical records.

The second alarm condition (possibly a more severe or urgently necessary medical situation) was predicted with an accuracy of almost 99.78%. Near-perfect accuracy in predicting this alarm condition illustrates the capability of the classifier to identify delicate nuances and correlated variations in the sensor data that indicate a distinct risk or health condition. The third alarm condition (life-threatening and requiring urgent treatment) was predicted with 100% accuracy. This outcome shows how well the classifier detected the most severe conditions (zero tolerance and high consequences for inaccurate predictions). In other words, accuracy in forecasting these situations has direct positive and negative implications for patients' survival, well-being, performance and more.

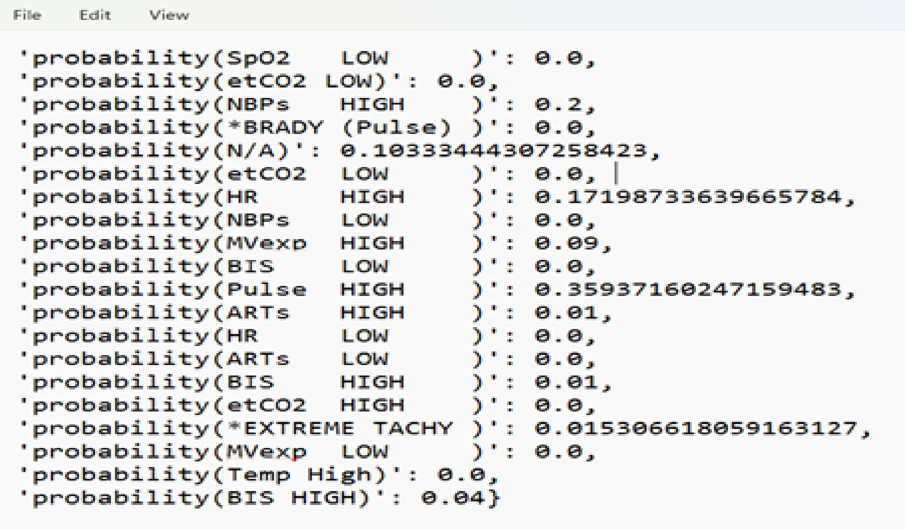
The average accuracy of 99.53% attained at all three alarm conditions is depicted. This figure combines the individual accuracies of all classifiers for each alarm condition and highlights the effectiveness and robustness of the Random Forest Classifier in our application domain. Predicting various alarms with an average accuracy greater than 99% from a pool of medical sensors can also provide further confidence in the adaptability of the above machine-learning approach in real-life medical healthcare applications.

6.2.4 Vital Sentinel: Adaptive Vital Sign Monitoring Architecture Using BCoT and Machine Learning

The novel architecture begins with the historical base information about past emergency room visits with patient demographic information and corresponding vital data to define a set of baseline ranges for the levels of various vital signs (e.g. heart rate [60-100 bpm]; blood pressure [110/70-140/90 mmHg]; and oxygen saturation [94-100%]). In real-time, data corresponding to input parameters about each new patient visiting the emergency room will be input into the system using IoT sensors deployed in the emergency room to continuously record vital signs to acquire current readings, prior readings corresponding to this same patient visit, and demographic information. The rate of change (such as fast and slow) will be calculated for each vital sign at a short time window.

The vital signs showing a significant change trend (possibly ever deteriorating or improving) will be given a higher weight. In comparison, those with no significant trend will be given a lower weight. For example, a heart rate rise by 15 bpm in 1 minute will receive a weight of 2, a faint blood pressure rise by five mmHg will receive a weight of 1, and when there is no significant change in an oxygen saturation reading will receive a low weight of 0.5. According to the above analytical method, adaptive thresholds will be calculated, combining the baseline value of each vital sign and the dynamically calculated weight (baseline values*weights of vital signs). They consider both the baseline range and the current trend. The data that surpass the adjusted threshold for a given vital sign will be flagged as a high priority, with the immediate decisions being taken or sent elsewhere. In contrast, those within or beneath the thresholds can be processed using a lower priority or sent for continuous monitoring.

Another component involves using a Random Forest model that trains against historical patient data and exports it to PMML format for deployment on edge nodes. This provides the capability for running predictions and inferencing on captured IoT sensor data on-device, thus enhancing the monitoring and decisions made about the new patient. Figure (27) shows a screenshot of the PMML execution output, demonstrating the integration of machine learning models into the system's decision-making process.



```
'probability(SpO2   LOW     )': 0.0,
'probability(etCO2 LOW)': 0.0,
'probability(NBPs   HIGH    )': 0.2,
'probability(*BRADY (Pulse) )': 0.0,
'probability(N/A)': 0.10333444307258423,
'probability(etCO2  LOW     )': 0.0,
'probability(HR     HIGH    )': 0.17198733639665784,
'probability(NBPs   LOW     )': 0.0,
'probability(MVexp  HIGH    )': 0.09,
'probability(BIS    LOW     )': 0.0,
'probability(Pulse  HIGH    )': 0.35937160247159483,
'probability(ARTs   HIGH    )': 0.01,
'probability(HR     LOW     )': 0.0,
'probability(ARTs   LOW     )': 0.0,
'probability(BIS    HIGH    )': 0.01,
'probability(etCO2  HIGH    )': 0.0,
'probability(*EXTREME TACHY )': 0.015306618059163127,
'probability(MVexp  LOW     )': 0.0,
'probability(Temp High)': 0.0,
'probability(BIS HIGH)': 0.04}
```

Figure (27): Screenshot of the PMML execution output.

6.2.5 Details of Vital Sentinel: AI and Blockchain Converge to Safeguard Life Architecture

The novel architecture utilises recent technologies to improve the tracking and early detection of clinical deterioration in emergency room patients. The high-level architecture includes edge computing, AI, IoT, and Blockchain technology for secure, intelligent data use. Below is an instruction that describes a task, paired with input that provides further context.

Historical Data Analysis

1. **Data Collection**: Historical data (determined to be relevant) from past emergency room cases is collected: demographic information (patient age, with or without medical history) and readings from other vital sign sensors.
2. **Baseline Establishment**: This information to help determine baseline normal ranges for vital signs, such as:
    - Heart Rate (HR): HIGH (60-100 bpm), LOW (60-100 bpm)
    - BRADY (Pulse): 50-120 bpm
    - Pulse: HIGH (50-120 bpm)
    - SpO2: LOW (90-100%)
    - etCO2: HIGH (30-50 mmHg), LOW (30-50 mmHg)
    - NBPs: HIGH (160/90 mmHg), LOW (90/50 mmHg)
    - ARTs: HIGH (160/90 mmHg), LOW (90/50 mmHg)
    - Range: 35...43 (36-39)
    - BIS: HIGH (20-70), LOW (20-70)
    - MVexp: HIGH (4.01-8.01 L/min), LOW (4.01-8.01 L/min)
    - EXTREME TACHY: 50-120 bpm

Real-time Patient Information Integration

1. **Sensor Deployment:** IoT sensors are placed in the emergency room to sense the patient's vital signs continuously.
2. **Data Acquisition:** Data readings indicate the current and historical readings (associated with that given patient visit), and different sensors continuously sense specific demographic information (associated with that given patient visit).

Dynamic Weighting Based on Trends

1. **Trend Calculation:** The system calculates the rate of change (positive or negative) for each vital sign over a short time window (e.g., last minute).
2. **Weight Assignment:** Higher weights are assigned to vital signs exhibiting significant positive or negative trends, indicating potential deterioration or improvement. For example:
   - Heart Rate (HR): Significant positive trend (an increase of 15 bpm in 1 minute). Assign high weight (e.g., 2).
   - Blood Pressure (BP): Slight positive trend (increase of 5 mmHg in both systolic and diastolic). Assign medium weight (e.g., 1).
   - Oxygen Saturation (SpO2): No significant trend (unchanged). Assign low weight (e.g., 0.5).

Adaptive Threshold Calculation

1. **Baseline and Weight Combination**: Combine the baseline value for each vital sign with the dynamically calculated weight to create an adaptive threshold. For example:
   - HR: Baseline (95 bpm) + (Weight * Trend) = 95 bpm + (2 * 15 bpm) = 125 bpm.
   - BP: Baseline Systolic (140 mmHg) + (Weight * Trend) = 140 mmHg + (1 * 5 mmHg) = 145 mmHg.
   - BP: Baseline Diastolic (90 mmHg) + (Weight * Trend) = 90 mmHg + (1 * 5 mmHg) = 95 mmHg.
   - SpO2: Baseline (98%) + (Weight * Trend) = 98% + (0.5 * 0%) = 98% (no significant change).

Data Prioritization and Alerting

1. **Threshold Evaluation**: The streamlined sensor data is evaluated against the adaptive thresholds.
2. **Flagging High-Priority Data**: Data exceeding the adjusted threshold for a specific vital sign is flagged as a high priority, triggering immediate action or further analysis.
3. Continuous Monitoring: Data within acceptable ranges (below the adaptive threshold) can be processed with lower priority or used for continuous monitoring.

Integration of Random Forest Classifier and PMML

1. **Model Training:** A Random Forest model uses historical patient data to classify and predict critical conditions. Features include heart rate, blood pressure, and oxygen saturation.
2. **PMML Export:** The trained Random Forest model is exported to the PMML format using libraries like Nyoka in Python or the PMML library in R.
3. **Deployment on Edge Nodes**: The PMML-based Random Forest model is deployed on edge nodes (e.g., Raspberry Pi devices) to enable on-device predictions and analysis of incoming IoT sensor data.
4. **Real-time Predictions:** As real-time vital sign data is collected and pre-processed, it is fed into the deployed Random Forest PMML model on the edge nodes. The model generates predictions about the likelihood of different alarm conditions based on the observed vital sign patterns.

AI-based Predictions and Insights

The novel architecture builds upon the Random Forest classifier, which can learn from historical patient data and make predictions and insights that can help support threshold-based adaptive monitoring. A trained Random Forest model is exported to PMML, and then the model is run on edge nodes in the form of RPi4 devices to deliver real-time inferences on the IoT sensor data.

1. **Alarm Condition Prediction:**

   As real-time vital sign data was collected and pre-processed, it was fed into the deployed Random Forest PMML model on the edge nodes. The model analysed the data and directly predicted the presence or absence of specific alarm conditions, such as tachycardia (rapid heart rate), hypoxemia (low oxygen saturation), or hypertensive crisis (severely elevated blood pressure). These predictions from the Random Forest model were used in conjunction with the adaptive threshold-based approach to provide a more comprehensive assessment of the patient's condition. For example, when the adaptive threshold analysis flagged a patient's heart rate as a high priority, and the Random Forest model also predicted the presence of tachycardia, this combined information triggered immediate intervention and escalation of care. This integrated approach leveraged machine learning predictions and traditional threshold-based monitoring to enhance the accuracy and timeliness of patient assessment in the edge-computing environment.
2. **Risk Scoring:**

The Random Forest model's predictions were utilized to calculate a risk score for each patient, indicating the overall likelihood of experiencing an alarm condition. This risk score was derived by combining the predicted probabilities of various alarm conditions, weighted by their severity or clinical significance. For instance, when the model predicted a 70% probability of tachycardia and a 30% probability of hypoxemia for a particular patient, the risk score was calculated by assigning appropriate weights to these conditions based on their severity and then combining the weighted probabilities. This risk score was then integrated with the adaptive threshold analysis to prioritize patients and allocate resources more effectively. Patients with higher risk scores were triaged and attended to more urgently, while those with lower risk scores were monitored closely or managed with lower priority. This approach allowed for a more nuanced and efficient allocation of healthcare resources based on the predicted risk levels of individual patients.

3. **Early Warning System:**

   By continuously monitoring the predictions from the Random Forest model, the system detected early warning signs of potential alarm conditions, even before the adaptive thresholds were exceeded. This proactive approach enabled healthcare professionals to intervene early and implement preventive measures, potentially averting or mitigating the severity of adverse events. The system's ability to analyse complex patterns in real-time data allowed for more accurate and timely identification of at-risk patients. Healthcare providers were able to prioritise their attention and resources more effectively, focusing on those patients most likely to experience complications. This early warning capability improved patient outcomes and contributed to more efficient resource allocation within the healthcare facility. Integrating machine learning algorithms with traditional monitoring systems demonstrated the potential for significant advancements in patient care and safety protocols.

   For example, if the model predicted an increasing probability of hypoxemia over time, even though the patient's oxygen saturation levels were within the adaptive threshold range, this could have triggered an early warning alert. Healthcare professionals could then investigate the cause, adjust oxygen therapy, or take other appropriate actions to prevent further deterioration. Integrating AI-based predictions and insights from the Random Forest model with the adaptive threshold-based monitoring approach created a robust and comprehensive system for intelligent vital sign monitoring in emergency rooms. This synergistic approach leveraged the strengths of both techniques, providing early warning capabilities, risk stratification, and enhanced decision support for healthcare professionals, ultimately leading to improved patient outcomes and more efficient resource allocation.

Secure Data Sharing and Transparency

1. **Alert Generation:** High-priority data triggers alerts shared with healthcare professionals via a private Blockchain network.
2. **Secure Data Sharing:** AI-generated insights and predictions from the Random Forest model are packaged as transactions and submitted to the Blockchain for secure, transparent, and immutable sharing among authorised stakeholders.

6.2.6 Power Cost

A step that is also very important in the proposed system is measuring the power consumed by the devices in several ways. Two approaches were used to calculate the power consumed by an RPi4. One is called the ‘clamped meter’, and the other uses the ‘top’ command prompt. Follow these steps for the ‘clamped meter’ approach: To calculate the power that the Pi consumes, clamp the meter around one power cable wire (usually the positive wire/red) and check the milliampere of the RPi4 draws (mA).

Power can be calculated as long as we know the voltage (the result is often 5V for RPi4). For the ‘top command’ method, enter the RPi4 terminal, run the top command, read the growing processes and CPU usage from the Head column, and estimate power consumption according to their CPU utilisation. This is because the more CPU usage there is, the higher the power consumption, although the precision of this method is indirect. Figure (28) details the system’s power consumption regarding workloads in five states: Idle Connection, Information Exchange, Mining, Model Execution, and all processes. Also, Figure (28) concludes that the idle connection drains less power than the processes of Mining or Model Execution, which requires more energy. The voltage of the RPi4 at those different states did not change much in 5V, indicating that the power supply is stable to prevent variation of the RPi’s voltage output; this helps to balance the system performance.

The current is proportional to activity, starting at 0.9 A in Idle Connection and rising to 1.4 A at Mining and Model Execution. This relation between the workload and the current draw can be explained because more energy will be drained as the activity increases. Accordingly, the power consumption increases as well by using more current. This can be noticed at Idle Connection energy consumption of 4.5W, which rises to 7W at Mining and Model Execution.

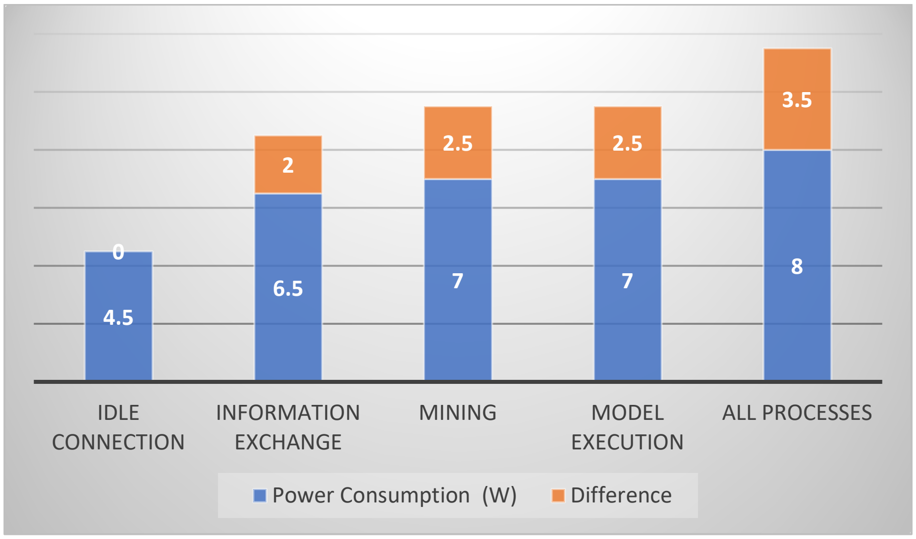


Figure (28): Power consumption at different stats.

The type of operation tasks can also influence power consumption. For example, information exchange can increase power consumption by 2W compared to the idle connection state, and AI prediction or Blockchain mining tasks can lead to a 2.5W increase. However, this impact can be mitigated by the strategic distribution of workloads among network nodes. By ensuring that each device does not need to complete all daily tasks, workloads can be shared and better distributed, leading to a sustainable reduction in power consumption. This highlights the potential for the audience to manage and reduce power consumption in their RPi4 devices actively.

6.3 System Analysis

The proposed architecture is secure, highly robust, scalable, and efficient regarding power consumption and model accuracy to support AI-enabled IoT applications at the edge. Continuous AI prediction can be ensured to remove a signal point of failure and provide government agencies and organisations with the processed data and outcomes for better decision-making. Data integrity is guaranteed by verifying and sealing all AI data (Inputs and Outcomes) on a secure, decentralised, and transparent Blockchain platform. An integrated architecture involving AI, IoT, and Blockchain can be deployed in this network.

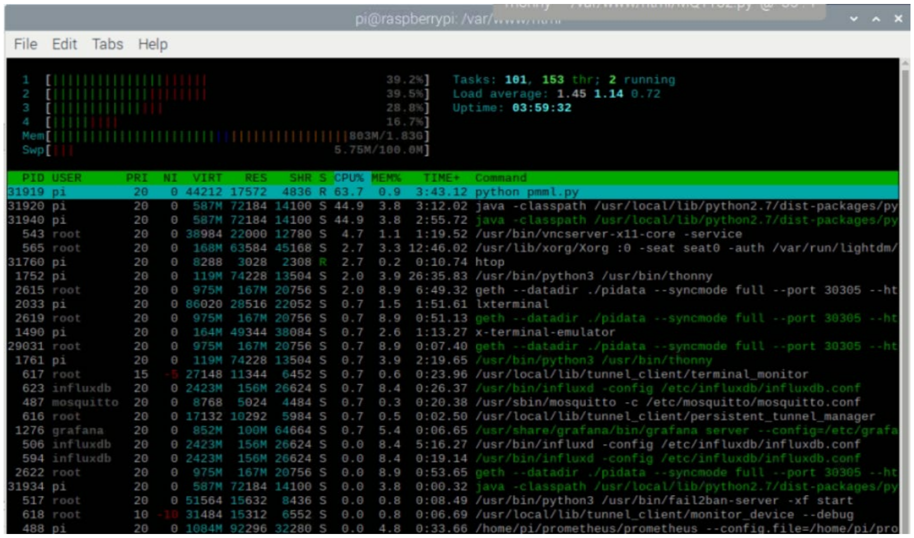
IoT sensors are deployed across distant locations, such as patients' rooms, to harvest critical real-time data such as vital signs, patients, and environmental conditions. This data is continuously streamed to the edge nodes, and the RPi4 nodes act as computational resources along with AI capabilities. The AI classification model trained from patient data in the past is ready to be deployed using the PMML file format. These RPi4 nodes have a trained model that can be used for on-device prediction and analysis of the incoming data streaming in from the IoT sensors. Lower latency and real-time response times are achieved by processing and making predictions at the edge closest to the source, which is required in any emergency room setting. Using edge nodes and IoT sensors, input data are processed and continuously streamed to the RPi4 nodes. The nodes powered by the AI classification models (which are deployed as a PMML file) analyse the incoming data to generate predictions. AI insights and recommendations based on the trained model are then securely shared over a private Blockchain network to ensure data integrity, trust, and confidence among the stakeholders.

In the Blockchain network, block validations are done by many nodes, which add a new block with valid transactions to the distributed ledger. Moving to the Core, the central part of the system. The access and interaction with the Blockchain occur using robust identity management, authentication, and authorisation mechanisms so that only the approved entities can join the network and access the shared data. The data flow starts from the IoT sensors that acquire data from Emergency Rooms and send the sensory data to the edge nodes using the secure publish-subscribe MQTT protocol. The prediction models are packaged into edge nodes that run a logic machine learning model based on PMML in the edge nodes. The edge nodes process sensory data, and the AI models give predictions and insights. The AI-generated insights would be built on top of the necessary transactions and submitted to the private Blockchain network. In addition, the transactions are first validated and approved by Blockchain nodes before being added to the distributed ledgers. Authorised stakeholders, such as healthcare professionals (e.g., doctors), can access the shared data by retrieving it from the Blockchain network. By putting the AI-based decisions on the Blockchain network, everyone can access the same data, and the decisions are jointly taken and authenticated. Those interactions increase the trust in smart IT investments, enhancing patient outcomes and improving healthcare operations. IoT, edge computing, and Blockchain work harmoniously in this system to offer secured, intelligent, and decentralised data management in the Emergency Rooms. Edge computing provides low latency and timely responsiveness for the system. On the other hand, the Blockchain provides different benefits such as data integrity, transparency, and trust among stakeholders.

The RPi4 multi-threaded processing power is increased, plus the overall system responsiveness for multi-tasking can multi-fold compared to old single-board computers within the RPi4 family. This machine can handle tons of tasks at the same time and spread out the work between its cores. This works incredibly well for programs that run multiple processes simultaneously. Another example is the operating system acting as a conductor, issuing instructions onto which cores should run which tasks so they can play simultaneously and in harmony. The programs or applications are the instruments, the cores are the conductors, and the players are the workloads. Special tools, such as ‘top’ and ‘htop’, can be used to track CPU usage, and utilisation can be observed to see what program hogs more than other programs.

While the ‘top’ command provides a handy tool for inspecting processes, the ‘htop’ command on an RPi4 provides a more straightforward and intuitive way to monitor the resources used. Due to the extensive use of graphical visualisation, it is much easier to immediately understand the resources used, with colour bars and well-label fields. An excerpt of the htop command run on the system is shown in Figure (29). As can be seen from the figure, the htop command provided real-time outputs showing the usage of various resources in the system. Some fields shown include the individual process being run on the system along with parameters such as the CPU and memory usage, the process ID, and the uptime (i.e., how long the process has been running). The nature of this command allows us to quickly sort the processes according to various parameters like CPU usage and memory usage by clicking on the column headers. The names of different processes can also be filtered to help isolate processing tasks of interest.

In the current system scenario, the ‘htop’ command output indicates that the current system load is not high. All memory is seemingly free, while the 4-core CPU usage is currently only at 39%, 39%, 28%, and 18%, and only takes up 800MB out of 2GB of memory. The system is currently healthy. However, suppose any individual number of one of the above parameters is high. In that case, more than 50% of the total or a particular process uses too much CPU, and the cause of the blockage can be easily diagnosed using htop output. Steps can be taken to reduce the workload of the process (e.g. optimise the code) or stop the process if necessary. By optimising the code utilising all the features of Python, such as vectorised array operations and assignments, it is often possible to significantly improve the efficiency of a process.



```
  1  [|||||||||||||||||||||                    39.2%]   Tasks: 101, 153 thr; 2 running
  2  [|||||||||||||||||||||                    39.5%]   Load average: 1.45 1.14 0.72
  3  [||||||||||||||||                         28.8%]   Uptime: 03:59:32
  4  [|||||||||                                16.7%]
  Mem[|||||||||||||||||||||||||||||||||||||||803M/1.83G]
  Swp[|||                                5.75M/100.0M]

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
31919 pi         20   0 44212 17572  4836 R 63.7  0.9  3:43.12 python pmml.py
31920 pi         20   0  587M 72184 14100 S 44.9  3.8  3:12.02 java -classpath /usr/local/lib/python2.7/dist-packages/py
31940 pi         20   0  587M 72184 14100 S 44.9  3.8  2:55.72 java -classpath /usr/local/lib/python2.7/dist-packages/py
  543 root       20   0 38984 22000 12780 S  4.7  1.1  1:19.52 /usr/bin/vncserver-x11-core -service
  565 root       20   0  168M 63584 45168 S  2.7  3.3 12:46.02 /usr/lib/xorg/Xorg :0 -seat seat0 -auth /var/run/lightdm/
31760 pi         20   0  8288  3028  2308 R  2.7  0.2  0:10.74 htop
 1752 pi         20   0  119M 74228 13504 S  2.0  3.9 26:35.83 /usr/bin/python3 /usr/bin/thonny
 2615 root       20   0  975M  167M 20756 S  2.0  8.9  6:49.32 geth --datadir ./pidata --syncmode full --port 30305 --ht
 2033 pi         20   0 86020 28516 22052 S  0.7  1.5  1:51.61 lxterminal
 2619 root       20   0  975M  167M 20756 S  0.7  8.9  0:51.13 geth --datadir ./pidata --syncmode full --port 30305 --ht
 1490 pi         20   0  164M 49344 38084 S  0.7  2.6  1:13.27 x-terminal-emulator
29031 root       20   0  975M  167M 20756 S  0.7  8.9  0:07.40 geth --datadir ./pidata --syncmode full --port 30305 --ht
 1761 pi         20   0  119M 74228 13504 S  0.7  3.9  2:19.65 /usr/bin/python3 /usr/bin/thonny
  617 root       15  -5 27148 11344  6452 S  0.7  0.6  0:23.96 /usr/local/lib/tunnel_client/terminal_monitor
  623 influxdb   20   0 2423M  156M 26624 S  0.7  8.4  0:26.37 /usr/bin/influxd -config /etc/influxdb/influxdb.conf
  487 mosquitto  20   0  8768  5024  4484 S  0.7  0.3  0:20.38 /usr/sbin/mosquitto -c /etc/mosquitto/mosquitto.conf
  616 root       20   0 17132 10292  5984 S  0.7  0.5  0:02.50 /usr/local/lib/tunnel_client/persistent_tunnel_manager
 1276 grafana    20   0  852M  100M 64664 S  0.7  5.4  0:06.65 /usr/share/grafana/bin/grafana server --config=/etc/grafa
  506 influxdb   20   0 2423M  156M 26624 S  0.0  8.4  5:16.27 /usr/bin/influxd -config /etc/influxdb/influxdb.conf
  594 influxdb   20   0 2423M  156M 26624 S  0.0  8.4  0:19.14 /usr/bin/influxd -config /etc/influxdb/influxdb.conf
 2622 root       20   0  975M  167M 20756 S  0.0  8.9  0:53.65 geth --datadir ./pidata --syncmode full --port 30305 --ht
31934 pi         20   0  587M 72184 14100 S  0.0  3.8  0:00.32 java -classpath /usr/local/lib/python2.7/dist-packages/py
  517 root       20   0 51564 15632  8436 S  0.0  0.8  0:08.49 /usr/bin/python3 /usr/bin/fail2ban-server -xf start
  618 root       10 -10 31484 15312  6552 S  0.0  0.8  0:06.69 /usr/local/lib/tunnel_client/monitor_device --debug
  488 pi         20   0 1084M 92296 32280 S  0.0  4.8  0:33.66 /home/pi/prometheus/prometheus --config.file=/home/pi/pro
```

Figure (29): CPU usage using the ‘top’ command tool in RPi4.

Memory-wise, the RPi4 has multiple configurations – from an affordable 1 GB to an 8 GB model. The RPi4 consumes about 5 W in an idle state, with CPU usage at around 5-10%. When running heavyweight programs, the power usage goes up to 7 W, and CPU usage increases to 50-70%, depending on the workload. The choice of RAM allows as many programs as possible to run simultaneously without slowing down. In addition to RAM, fast memory bandwidth is required. Memory bandwidth refers to the amount of data passing between the CPU and RAM. The faster this bandwidth, the more quickly the program can manipulate the RAM, which speeds up overall performance. In Addition, the operating system implements memory management so that no single program can claim the entire amount of available RAM.

Geth Metrics – an inherent feature of the Ethereum infrastructure – provides several optional metrics like meters, timers, counters, and gauges, each offering a different way of tracking various aspects of Geth’s network performance and resource consumption. Meters track the cumulative number of occurrences and their pace of growth over time, providing an understanding of Geth's activity levels across several areas. Timers track events by measuring their completion time, offering percentile-based duration data, and helping uncover possible bottlenecks. Counters keep track of specific actions, such as opening connections or determining the number of database queries. Gauges track dynamically changing values such as current memory utilisation or the number of connected peers. Metrics can improve Blockchain performance by tracking what is consuming the most resources, how long processes take to complete, and understanding how to mitigate and improve certain aspects of network performance. From Geth, metrics can be exported to InfluxDB and offered in the Prometheus format, with the intent of viewing such metrics data with Grafana to understand what is happening under the hood of Geth. Geth can export metrics as an InfluxDB file, which will import them into the time-series database InfluxDB, or in the famous Prometheus-formatted metrics (a text format that allows for easy spread across servers and discs) that can then be read and displayed using the free and widely used Grafana software.

Disk space used, memory used, and CPU utilisation are some of the performance parameters supporting the network. Counters monitoring disk performance are informative and essential for the health and performance of storage systems. The counters called 'Disk Read Data' and 'Disk Write Data' respectively indicate the average amount of data transferred while the disk domain performs the read versus the write operations. The counters 'Disk Reads/sec' and 'Disk Writes/sec' quantify the number of the corresponding operations per second. Monitoring these counters allows system administrators to detect trends in disk activity, areas of concern and opportunities for optimisation.

Figure (30) illustrates the disk read and write operations before and after the transactions and mining process start in Geth. Before the transactions and mining process begins, the disk read and write operations are low. Geth only loads the necessary data from the Blockchain database for the following transactions and mining processes. Once the transactions and mining process commences, the disk read and write operations increase significantly. Geth is now actively reading and updating the data from the Blockchain database. The disk write operations are mostly higher than disk read operations because Geth constantly writes new data to the Blockchain database while the transactions are processed, and the blocks are mined. As the figure shows, disk read and write operations are prone to change dramatically over time. This is because the number of transactions and the size of the blocks can drastically vary. For instance, if new transactions are suddenly submitted to the network, the disk read and write operations will dramatically increase.

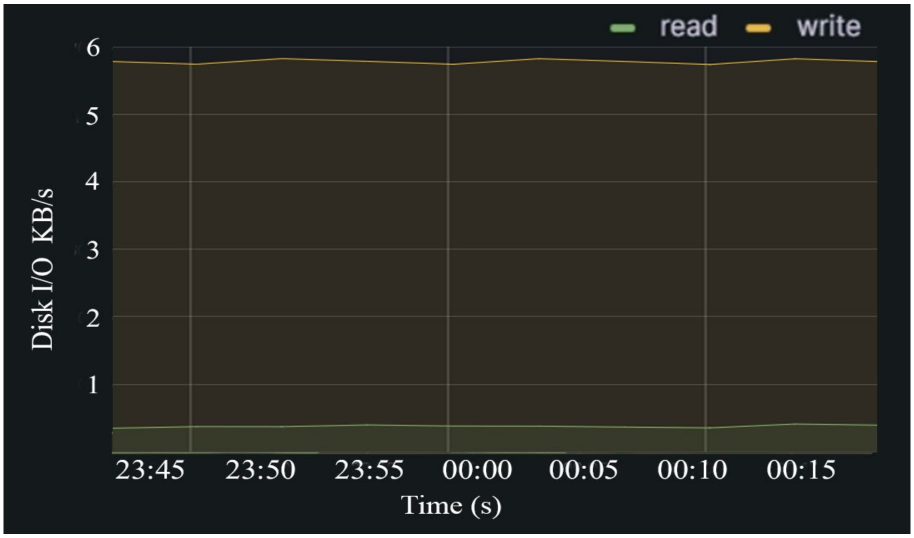


Figure (30): Disk I/O performance in the proposed novel architecture.

Figure (31) describes approximately the memory usage; the RPi4 node uses about 125 MB to 150 MB of memory to mine, whereas the memory usage increases massively once the AI mode of classification starts being turned on, giving impetus to the AI to be able to predict and analyse the incoming transactions on-device in addition of submitted transactions being added, therefore loaded additional data into memory to processes transactions, for any Blockchain database, transaction pool, and account state. Furthermore, memory usage, which is more appropriate to be volatile, could rise and fall significantly over time because the number and size of transactions can vary significantly. Geth might have to load additional information into memory to process transactions. The peak memory usage is around 200 MB - most likely because Geth is now mining many transactions; the memory usage then slightly down-chucked once Geth finished some of the processing transactions. However, memory usage is still above normal as Geth process new transactions and maintains the Blockchain database.

Furthermore, Figure (31) gives an overview of memory usage after sending the transaction. This information could be used to troubleshoot performance problems and give a chance for optimisation. Here, the value of memory usage rises gradually; the figure shows that Geth continuously loads more data into memory. At the same time, several spikes in memory usage could be seen, which correspond to the times when Geth processes a lot more transactions. After some time, memory usage seems to stabilise, suggesting that Geth reached a steady state where it deals with new transactions by freeing up unused memory.

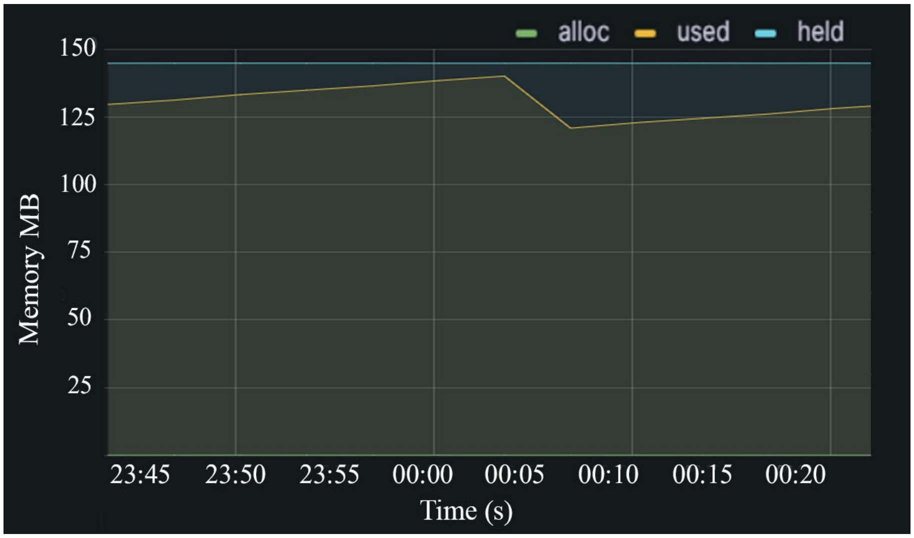


Figure (31): Memory performance in the proposed novel architecture.

Similarly, the actual CPU utilisation of each node is shown in Figure (32). The actual CPU utilisation of RPi4 nodes is less than 26 %. On the other hand, CPU utilisation of the thinking process is about 100% on RPi4 because, in the mining process, CPU utilisation is almost 100% of 400% RPi4 Cores. Actual CPU utilisation is increasing slowly because the Geth dashboard command performs average CPU time with elapsed time since it was booted. From a long view, the Rpi4 node's CPU usage is stable. Figure (24) illustrates that CPU usage drastically increases after running the AI classification model, admitting device predictions, analysing incoming data, and submitting transactions. This is mainly because the Geth and classifier model that was created both need additional CPU usage to run the transactions, like when validating a transaction, updating the Blockchain database, and syncing the database in the network. CPU usage shows periodic spikes related to times when Geth mainly processes more than one or more complex transaction. CPU usage is underrun later, showing that Geth reached the steady state of processing new transactions and freeing the extra CPU run time. Furthermore, the CPU usage is going up continuously in the last frame of time, which includes many transactions that need Geth to run to maintain the high requests. Furthermore, there are a couple of spikes in which the CPU is going up, likely when Geth is processing more transactions and requires more CPU cycles to process and verify the transaction. CPU usage is later underrun, which indicates Geth reached the steady state of inserting new transactions and freeing more CPU resources that are not in use.

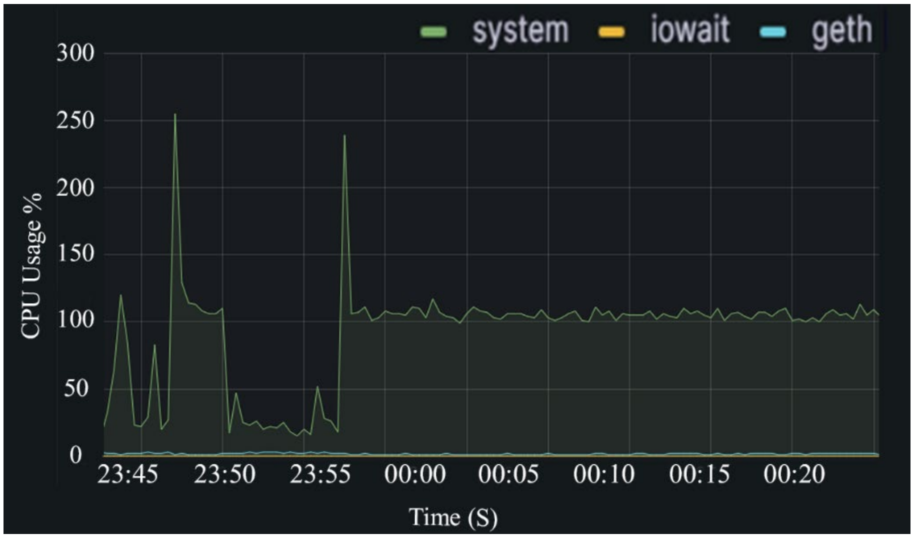


Figure (32): CPU performance in the proposed novel architecture.

6.4 Chapter Summary

A comprehensive architecture has been developed to harness the benefits of four pivotal emerging technologies: edge computing, Blockchain, AI, and IoT. This research delves into the potential of merging these technologies into a unified platform to enhance the accuracy of IoT data collection within intensive care units (ICUs). The findings reveal that the overall accuracy of IoT data reaches an impressive 99.53% across three distinct alarm conditions.

The architecture emphasises security by implementing robust Blockchain technology, which serves as a public platform to disseminate AI advantages through an edge computing layer. This edge layer is designed to provide a secure framework that can sense, analyse, reason, and act—setting a new standard for data-intensive applications. Additionally, the system demonstrates its capability to predict outcomes based on medical vital signs datasets, achieving a reliable level of accuracy while maintaining acceptable latency for real-time applications.

Furthermore, the architecture was evaluated in terms of the impact of power sources on the utilised devices. Results indicate that low-cost and low-power IoT devices can be effectively deployed to meet the demands of AI and Blockchain within a network comprising several hundred fixed nodes. This showcases the feasibility of integrating these technologies to create a secure, intelligent, and highly efficient platform applicable in various contexts, including monitoring and analysing vital signs data. The edge computing segment is crucial as it enables real-time data storage, processing, and analysis with minimal latency near data collection points.

Blockchain technology enhances this framework by offering a secure and transparent mechanism for sharing and processing decentralised data from multiple sources. The system is built upon low-cost and low-power IoT devices, making it adaptable across diverse application areas, especially in environments where resource utilisation is strictly regulated. This innovative architecture addresses existing challenges and paves the way for future advancements in healthcare monitoring systems and beyond.

In the next chapter 7: Performance Analysis of BCoT Applications, a crucial factor is how to monitor the performance of the integration of IoT and Blockchain. The performance monitoring of IoT-Blockchain is introduced in Chapter 7. Firstly, the challenges and bottlenecks of the performance monitoring for IoT-Blockchain are presented, then the protocols and tools for the performance monitoring are summarised and followed by the results being analysed. Furthermore, the integration of private Ethereum Blockchains and IPFS will be covered with a focus on how to increase the scalability, security, and trustability.

Chapter 7

Performance Analyses of BCoT Application

7.1 Introduction

The ‘state’ of the Ethereum Blockchain is what it means for the transaction machine to be at that moment. It includes the account balances, the data in all the existing smart contracts, conditions for future transactions, and anything else. Any node operating as part of the Ethereum network from this state may submit a transaction that modifies the state. The submitted transaction is held in the submitter’s local memory and broadcast to every other node in the network using a P2P communication protocol. For instance, each node has a transaction pool (called txpool) that holds incoming transactions until they are validated. New block candidates are instantiated by recognised mining nodes inserting a transaction set from the txpool. Consensus is reached: the network votes to accept the new block through a consensus protocol, such as the PoA protocol. This is an alternative to the energy-intensive PoW algorithm widely used in the original Ethereum implementation. Once the block is created and accepted by reaching a consensus, it is sent to all other nodes. The receipt node removes the validated transactions from its local txpool and adds the validated block to its local Blockchain database. Each node’s Blockchain is updated to a consistent state: all transactions are confirmed and replicated. This is how we achieve data integrity. Ethereum officially ships a node implementation called Geth (Go-ethereum). It implements the Devp2p (Node Discovery Protocol) and RLPx (Rail Layer Protocol), which are the P2P protocols used within the Ethereum network for discovering nodes, network communication and RLP data transmission. Geth uses UDP and TCP to send and receive data over the internet.

7.2 Integration of IoT with Ethereum Blockchain (BCoT)

Using Blockchain to integrate the IoT seems feasible because this technology can potentially resolve many issues related to device interconnectivity and management, data and user privacy, and network, data, and device security. However, it is essential to remember that there are inherent limitations in the number and type of functions an IoT device can perform based on processing power and battery power and that scalability and latency issues, often attributed to Blockchain technology, need to be considered. Any realisation of the potential of integrating Blockchain with the IoT implies balancing Blockchain's highly desirable security and privacy benefits and the realistic limitations of resource-constrained IoT devices. This requires imagination, research, and joint effort among technology stakeholders to build a healthy ecosystem in which economic, technical, social and governance considerations offer a path toward the responsible use of technology (Zubaydi, et al., 2023).

Efforts in integrating Blockchain-IoT need to focus on finding solutions that leverage the benefits of Blockchain technology, such as lightweight Blockchain implementations optimised for IoT, effective data management solutions, and techniques for offloading heavy computational workloads to more robust devices on the cloud, while considering the resource constraints of IoT devices. These potential merits render the combination of Blockchain and IoT most attractive in advancing IoT and Blockchain technology, which is why research in this direction is ongoing. The research addresses related issues, from adapting the Blockchain platform, distributing trust and processing workloads, programmability of distributed systems, and security aspects such as replay and Sybil attacks to global-scale applications and deployment considerations. With these explorations, the research in IoT and Blockchain approaches one of the most promising examples of a symbiotic relationship: bringing us closer to a future where innovation in how we connect, control and secure devices and IoT data in a hyper-connected world is disruptive because it is effective and fosters trust (Aitizaz, et al., 2022)

However, the core of this research contribution is system design, programming, and implementation, as well as the use of smart contracts to coordinate and automate system implementation.

7.2.1 Node Discovery Protocol

The Ethereum network employs a DHT protocol inspired by Kademlia for peer discovery and content dissemination across its P2P infrastructure. In private Ethereum Blockchain implementations, nodes are manually integrated into the network, and a Kademlia-derived node discovery mechanism for peer routing is utilised. Each node is assigned a unique 256-

bit identifier, a 'node ID', generated using the Secp256k1 elliptic curve cryptography. The protocol defines inter-node distance as two node IDs' exclusive OR (XOR). Nodes maintain Ethereum Node Records (ENRs) containing current information about themselves and their neighbouring nodes.

A node's routing table stores information about its neighbours, organised into multiple k-buckets based on distance metrics. The current implementation utilises k = 16. Within these k-buckets, node entries are maintained in sorted order, with the most recently updated entries positioned at the tail and the least recently updated at the head. This decentralised approach to node discovery and routing enhances the network's resilience and efficiency in content storage and sharing across the P2P network. The system's design facilitates dynamic peer management and optimises network topology for improved performance and scalability (Eisenbarth, et al., 2022) (Jean-Philippe, et al., 2023).

7.2.2 The RLPx Transport Power Protocol

RLPx is a network transport protocol derived from TCP, designed to enable communication between Ethereum nodes. It facilitates the transfer of encoded and serialized data in a manner that is both encrypted and authenticated. To establish a session, two nodes engage in a two-phase handshake process before exchanging critical messages. During this handshake, they share their public keys to ensure that messages are encrypted and authenticated. Once the handshake is complete, they negotiate further capabilities using a Hello message, which is exchanged upon receiving the initial handshake message. The foundation of this process is an RLPx Connection, which is established by forming a TCP connection and negotiating an ephemeral key pair for secure communication in the future. To illustrate the RLPx protocol, consider the following scenario: the initiator creates an ephemeral key using a shared secret and sends this encrypted secret to the recipient via an auth message. The recipient then uses the shared secret to generate the same key from the ephemeral key and responds with an auth-ack message. All messages exchanged after the initial handshake are framed. After negotiating the ephemeral key, both clients send a Hello message followed by a disconnect message, as they will eventually disconnect. During disconnection, the sender encodes a single byte of the reason code received by the network on the fragment.

7.2.3 Ethereum Wire Protocol

Based on the RLPx protocol, Ethereum defines several sub-protocols for different client conditions. The Ethereum Wire Protocol (ETH), used in this work, sees networks interconnected by full nodes sharing information about the Blockchain to update their respective ledgers. The Light Ethereum Sub-protocol (LES) is used by nodes and is defined as 'light', providing them full functionality to access the Blockchain safely. LES clients do not mine blocks; hence, they are not part of any consensus layer. A variation of LES for Parity Ethereum clients (Parity Light Protocol, PIP) was defined. We will refer to the ETH version eth/64 for this work. Nodes agree to use ETH and exchange Status messages containing the Total Difficulty (TD) and the hash of the latest block. Transactions are propagated similarly using one or more Transactions messages. For new blocks, nodes use NewBlock and NewBlock Hashes messages to communicate with their neighbours. The entire block is sent to a small set of connected nodes, while the new block's hash is forwarded to the rest of the peers.

7.3 Novel BCoT Architecture Design

Blockchain solutions for IoT (BCoT) applications have been getting more and more attention in the last few years due to the intrinsic merits of Blockchain technology in facilitating the security, transparency, and decentralisation of IoT's applications. However, existing solutions have several limitations, including a lack of scalability, performance, and security (Nguyen, et al., 2024) (Dorri, et al., 2017) (Gerald, et al., 2022) (Sabrina, et al., 2022). Based on these limitations, an interoperable novel BCoT architecture have been designed and evaluated, as shown in Figure (33). each playing a crucial role in mining and propagating new blocks within a private Ethereum PoA Blockchain network. These nodes are configured to perform specific tasks based on their designated roles. As validators and signers, they are responsible for ensuring the integrity of transactions and adding verified blocks to the Blockchain. This setup allows for efficient block propagation and maintains the security and reliability of the network.

Each node is considered as one entity of a Blockchain. Multiple micro-controllers such as Arduino Nano, ESP32, ESP8266, and Raspberry Pi Pico W. All act as an interface, adding multiple sensors streaming data onto the Blockchain node using MQTT communication protocol. Afterwards, edge-computing techniques were set up and tested to process and store IoT data locally before recording it on the Blockchain.

An Ethereum PoA client also has been set up and implemented on all three nodes. The smart contract has been developed and optimised for IoT functionalities such as storing sensor data and controlling the actuators, as it is the most efficient and scalable solution.

PoA is to be used for integration between IoT and Blockchain, which has been evaluated as the most efficient and scalable solution. Node-RED, a visual programming tool, has been applied here to program the system's workflow using a dashboard and module. The workflow of sensors and actuators has been configured and established with the help of Node-RED. Additionally, Node-RED has been integrated with InfluxDB and Grafana modules to provide data visualisation and analysis. In Addition, IPFS is implementing a filing system to provide additional off-chain storage. The edge-computing techniques are used to process and locally store IoT data before they integrate the Blockchain.

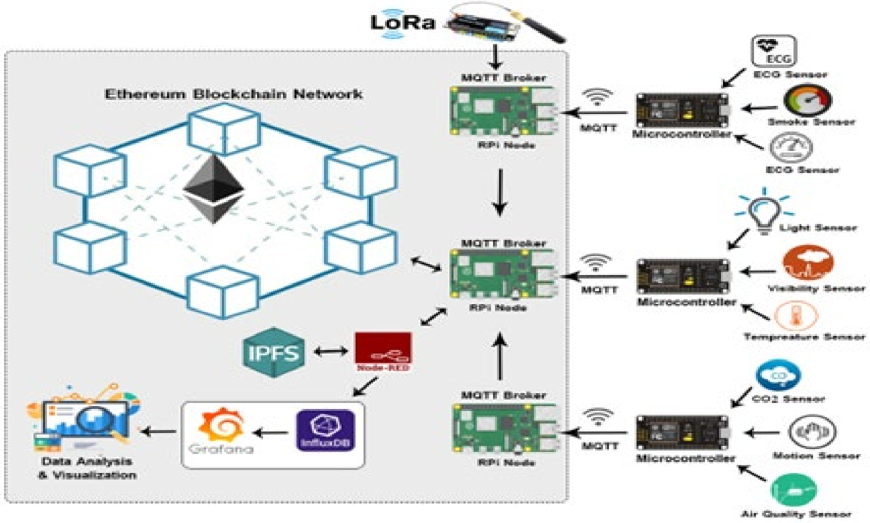


Figure (33): Proposed BCoT novel architecture design.

A scheme for Identity management, authentication, and access control was established for IoT devices that interact with the Blockchain to protect the security and privacy of IoT data. The first step was securing identity management for all devices. The immutability and robust framework of Blockchain make it an ideal data store for managing the identities of devices. In this work, we provided each device with a unique and unalterable identity stored on the Blockchain to authenticate and authorise it during its interactions in the network. Clear and practical steps were taken to secure the channel between source and destination. Authentication-based policies are implemented to secure communication between microcontrollers and the RPi4. To transfer sensor data from microcontrollers to RPi4, we used the MQTT protocol via the wolfMQTT library and Transport Layer Security (uTLS) protocol. The combination of wolfSSL and uTLS provided strong security; encryption and authentication were enforced to prevent eavesdroppers and man-in-the-middle attacks barred from decoding data whenever they tried to listen in or inject unauthorised content during the transit process. Access control for IoT via Blockchain involves setting unalterable rules that specify a user's eligibility to access resources within the network. On the Blockchain, rules are immutable, and thus, everybody (both legitimate network members and malicious actors) must agree to change them, which is virtually impossible. This approach further secured IoT by preventing the wrong entity from accessing network resources, tracing all access actions, and putting all access attempts in the public domain for audit.

The proposed novel architecture deployment was completed by programming the micro-controllers using Arduino IDE or Python and establishing communication with the nodes assigned according to the computing capabilities. Some RPi4 are designated validators and signers, i.e., for checking ethical transactions and adding new blocks to the Blockchain. The rest of the RPi4 devices have been configured to be regular nodes in the Blockchain network. The testbed was set to run for about three days, with each actor doing transactions every second and minute to have it look and operate as realistically as possible. Therefore, this enables the timeframe to adequately assess the statistics, metrics, and framework. To validate the collected data and check for potential issues, hourly averages or percentages for relative metrics were taken instead of depending on specific time measurements. Having the data checked for potential issues regarding the timing of data collection offers a complete picture for assessing the system. It would help further tune the design, configuration, and overall performance to suit the proposed IoT applications and use cases. Data from the sensors is picked up by the microcontrollers and then transmitted to the RPi4 network through the MQTT protocol.

Node-RED then published the data to the MQTT RPi4 broker to make the data available to other BCoT architecture components. This event kick-starts the asynchronous (nonblocking) data exchanges in the BCoT ecosystem and involved applications. The Node-RED workflows can be extended with custom integrations, providing Blockchain capabilities to the Node-RED application. Using that custom node, sensor data can be submitted to the Blockchain. The Node-RED application can perform transformations and validations to the data, store the data to IPFS, and store the content identifier for the saved file in the Blockchain. With this integration, the Node-RED application will save the sensor data (and possibly other data) to the IPFS decentralised storage network, and all the metadata associated with the saved file to the actual Blockchain. In this case, the sensor data and its data provider will be recorded as objects in the Blockchain network, potentially establishing complete trust in the innocent data. The Geth Metrics block provides a confirmation monitor for the Blockchain to ensure that the data will be immutable and provides catch-all errors and logging to provide an audit trail for troubleshooting. With this integration, sensor data (and possibly other sensor data) can be easily saved using the Blockchain and have the added security of being stored on a decentralised storage network and as verifiable metadata on an immutable Blockchain.

This data, and associated timestamps, was stored in InfluxDB, a purpose-built time series database, so it can be instantly searched, retrieved, and analysed for 'historical' data from which trends can be derived – which often helps when optimising system operation based on real-time, comprehensive data logging. InfluxDB was then interfaced with Grafana, a powerful visualisation front-end, where all of the sensor data is extracted from and laid out in various forms (charts, graphs, and dashboards) gained from that robust database. This layer serves as a primary tool for those who continuously monitor the operation and status of the BCOT, letting them watch over key parameters to prevent any unwanted anomalies in the data.

Integration of IPFS adds a layer of distributed content management to the architecture. Furthermore, the proposed novel architecture became decentralised using IPFS and MQTT, Node-RED, InfluxDB and Grafana to add a layer of resilience, scale, and efficiency. Inherent in the IPFS distributed storage model, data is never lost because it gets replicated across the network of nodes, substantially increasing data availability and fault tolerance. Lastly, content-addressed storage enhances the robustness and resiliency of the BCoT system, and the composition of the IPFS Chaincode with an IPFS Docker image facilitates easy and seamless deployment and management of IPFS nodes as part of the system architecture. With the decision to incorporate IPFS, we can now securely store and retrieve data using the content-addressed addressing format of IPFS. The containerised IPFS nodes can interact with the system, and Node-RED manages the data flows to and from these nodes for storage and retrieval. At the same time, InfluxDB continues to work with time-series data storage, and Grafana serves as the user interface for interactive visualisation and analysis of the data. The 'proposed novel architecture using IPFS for decentralised storage' provides a single compact framework for addressing all the challenges involved with data management. Here, we have leveraged the inherent benefits of Blockchain domains such as distributed trust, decentralised control, security, and P2P transactions, the foundational MQTT communication protocol, and the distributed content-addressed storage capability of IPFS in this unified framework.

7.4 Methodology

7.4.1 Latency Characterisation

In the scope of the thesis, this chapter focuses on an IoT-based application in the context of a private Ethereum network and scenarios wherein some IoT devices (e.g., due to performance constraints) cannot perform mining. However, mining is required for the Blockchain to continue operating. To overcome this, a proposed novel architecture introduces an optimised network architecture for a private Ethereum network, utilising Raspberry Pi 4 devices as computing nodes. Instead of employing all nodes as signer nodes, a role-based approach is adopted to enhance efficiency and effectively utilise resources. Two of the Raspberry Pi devices are designated as dedicated network signer nodes. These specialised nodes, strategically placed within each household on the network, possess the computational capability to perform mining operations and record new transactions onto the Blockchain. In addition, a linear topology was chosen for the network where, instead of using a node discovery protocol, we manually configure the nodes with the static IP addresses of all other nodes in the network.

The proposed novel architecture aims to build a new round of Ethereum chain-based networks based on Raspberry Pi devices. The Raspberry Pi operates as a node of the Ethereum network, helping to record, store, check and respond to the requests of other users. By combining a lightweight client, such as ‘Geth’, which requires less Blockchain data to be stored, with a reduction in the size of the Blockchain data to be stored and synchronised, we have minimised the computational impact on the non-signing node, as well as the resources (both electricity and information bandwidth) required for displaying the Blockchain information to those not involved. This network connectivity is accomplished bottom-up through what is known in software engineering as ‘handshaking’, a process in which each node explicitly defines the topological, or network, structure. Each Raspberry Pi maintains, in effect, a TCP connection open with each other RPi4 in the network. Furthermore, the architecture employs the Kademlia DHT protocol, in which each Raspberry Pi shares its k-bucket table with all other nodes in the network. This allows the network nodes to maintain a clear picture of the network topography, giving them the knowledge to share data efficiently. This novel architecture bundles lightweight clients, a Codec that reduces the amount of data stored, direct node-to-node connectivity, and the Kademlia DHT protocol to power a scalable and low-energy Ethereum Blockchain mesh of resource-constrained edge nodes such as RPis.

To bootstrap these Blockchain connections and gain consensus on which nodes should share what data, the Ethereum (ETH) protocol is brought to life on the network. IoT devices or other network participants transmit their transactions to signer nodes, which authenticate and add them to the Blockchain. The predetermined chosen nodes, or ‘signer nodes’, validate pending transactions and new blocks for the Blockchain. All validated transactions and the newly created blocks get distributed back to the network using the links created with the born RPi4 nodes. Thus, all nodes should have the new blocks and the latest transformation of the Blockchain. This novel design takes advantage of the strengths of the RPi4 devices while optimising resource usage and network efficiency. Specific nodes are assigned to sign and validate blocks to ensure everyone stays on the same page, and lightweight clients are featured for the non-signing nodes. This architecture allows for consistency between Blockchains, achieves security and reduces the overuse of resources in the network, thus employing the RPi4s for a private Ethereum network with pre-known, trusted participants.

A PoA consensus mechanism's transaction lifecycle differs slightly from a PoW's. The transaction lifecycle refers to the three steps in the life of a transaction, from the time it is added to the transaction pool until it is considered committed. This starts with submitting transactions to the transaction pool and broadcasting those transactions to the validator nodes (nodes which have been pre-approved to do validations in PoA). For PoA, it is not a computationally intensive algorithm run by the mining nodes (equivalent to validator nodes in PoA) as PoW, but rather validation using pre-approved identities of the controller nodes to create a new block containing the pending transactions and seal it. Moreover, when a validator node generates a new block that is considered acceptable by consensus and is successfully sealed on the chain, the new block is propagated throughout the network, where it gets verified by the network nodes. Upon successful verification, the transactions in the block will become effective and are committed and recorded on the Blockchain forever. In this context, there are two processes: transaction and block propagation on the Ethereum private network. The transaction propagation cascading process here is called the 'transaction-oriented latency'. The block propagation cascading process is called 'block-oriented latency'. On the other side of the transaction lifecycle, submissions and travelling blocks are carried out by the Ethereum client software such as Geth. By analysing the Geth log at its highest verbosity level (--verbosity 5), an insight gained into the workflow of transaction propagation and block propagation processes, as well as explore the transaction lifecycle in a PoA based Ethereum private network.

7.4.1.1 Transaction latency

In PoA Ethereum networks, transaction propagation and processing resemble many aspects of other types of consensuses. A transaction's life includes several discrete phases, each of which is important to the integrity of its network.

When a node receives the inbound transaction, it is queued for validation. Once this step is complete, it moves to a holding list, sometimes called the transaction pool, which acts as a holding stage. In this list, it is possible to see that multiple transactions have been collected before they are sent to a block in Ethereum. Once validated, the node spreads, sending the transaction to its peer network, which consists of other validator nodes. It does this through a special protocol for Transaction messages. The peer nodes receive and add the incoming transaction to their corresponding queues in the special storage block containing new, pending transactions. Next, the peer node validates and checks the transaction itself. If all checks pass, the transaction gets promoted out of the queue and into active status. It is added to the peer's transaction pool for further processing and block inclusion. This multi-stage process ensures a robust and decentralised approach to transaction management within the PoA Ethereum ecosystem, facilitating efficient and secure operations across the network.

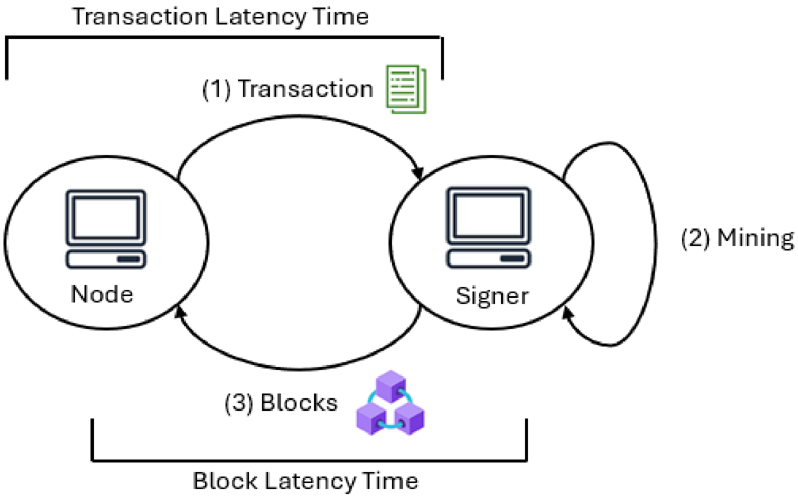


Figure (34): Lifecycle of transactions in the Ethereum Blockchain network.

A peer node does the same thing about this transaction, which will again be delivered to the rest of the PoA network. Transaction Latency of a PoA network can be formally defined as the time delay between when a transaction is sent out by a sender node to a peer node and when the validated transaction is brought up to the peer's transaction pool, as shown in Figure (34).

The lower the Transaction Latency, the quicker the transaction, once submitted, will reach the entire PoA network and be transacted upon, that is, accepted and validated by the set of authorised validator nodes. Transaction Latency is an important metric when executing or verifying transactions on a PoA-style Ethereum pseudo-peer-to-peer private network.

7.4.1.2 Block Latency

Block propagation and validation involve a complex interplay of nodes and transactions in Blockchain networks. The sequence commences when a mining node selects a subset of transactions from the transaction pool (txpool) and assembles them into a block. This newly mined potential block is then communicated to peer nodes via a NewBlock message. Upon receipt, the propagated block enters a queue at the recipient node. Subsequently, the block undergoes importation and processing by the peer node. This processed block is then transmitted to additional nodes within the network, perpetuating the propagation cycle. Each node validates the block and incorporates it into its local database during this process. The propagation cycle concludes when the new chain segment, comprising the recently mined block, fully integrates into the network. To mitigate redundant transmissions, nodes announce their block ownership, preventing scenarios where multiple peers attempt to propagate the same block simultaneously.

A critical metric in this process is block latency, the temporal interval between a block's mining and its importation by peer nodes. This metric approximates the time required for a block to traverse various network hops during propagation. This intricate process ensures the distributed consensus and integrity of the Blockchain, facilitating the network's decentralized nature while maintaining synchronisation across all participating nodes.

7.5 Performance Analysis

7.5.1 Geth Metrics

Geth, a platform, offers a collection of optional user metrics. Most are turned off by default to save computational resources. A user can then enable those using some flags, and some are considered expensive metrics, requiring another flag. The design goal is to let the engineers add metrics quickly all over the code, thus allowing it to automatically collect and query every executed function and letting the user explore the visualised outcomes without any abstraction and embedding constructs.

Metric types

The Geth Metrics Dashboard is a portal into the inner workings of the Ethereum node. It displays a variety of metrics based on meters, timers, counters, and gauges. Collectively, this information helps monitor Geth's performance and health.

Meters: Each measure a ‘thing’ that happens, the rate at which it happens, and how many times that rate has occurred over the last day. The meters are all digital odometers continuously updated every microsecond with each new event that enters the node. Each meter registers the total number of events, the average rate since the meter’s counter was first initialised, and the degree to which the node was busy within the past 1, 5 and 15 minutes.

Timers: Taking meters a step further, timers record the length of events, including percentiles (5th, 20th, 50th, 80th, 95th) – we can think of these percentiles as thresholds that measure the duration of certain events. For instance, events that are speedy form our 5th percentile, while fast but less frequent events form our 20th percentile; similarly, relatively fast events and their distribution is roughly symmetrical (i.e., 50 per cent below and 50 per cent above the median) form our 50th percentile, and the 80th or 95th percentiles include slower but still frequent events that probably deserve some alleviation.

Counters: These are simple counters that use a single integer field to keep track of something arranged. To see the current value, one needs to write a query to the dashboard anytime.

Gauges: Like counters, gauges track a single integer value with extra flexibility. They can be incremented, decremented, or set directly, providing a dynamic view of specific metrics of the running Geth node. Properly utilising these different metric types, a Geth Metrics Dashboard can help develop a clear picture of the node's status, identify areas of possible slowdowns, and keep the node running smoothly on the Ethereum network.

7.5.2 Performance Evaluation Process

To evaluate the real-time performance of the proposed BCoT architecture, the IoT data was exchanged at the Blockchain node, and the process, as depicted in Figure (35), was performed.

While the IoT data was processed, the Geth metric was presented. The purpose was to assess the system's performance as the CPU usage of the node, allocation of the node memory, disc I/O, latency, and throughput of node transactions have been allocated.

Geth's standard metric used to monitor metrics that include:

- The network traffic calculates the traffic volume, including in or out. This indicates the volume of incoming and outgoing packets at the Geth node.
- The block processed in time is considered a metric, which shows the time the Geth node needed to process the block.

- Network connection that indicates the number of network connections with the Geth node that was created.

These metrics are imported for monitoring the Geth node's health and performance, where it will detect when it fails.

The evaluation process is achieved using Geth, a client implemented on the Ethereum platform. Geth is written in the programming language Go and comes with a built-in EVM that processes transactions and deploys smart contracts. Geth comes with some default metrics. By default, the metrics are disabled to leave computing overhead for the average user. However, enabling command-line arguments using the—-metrics flag when starting the node allows the user to enable detailed metrics.

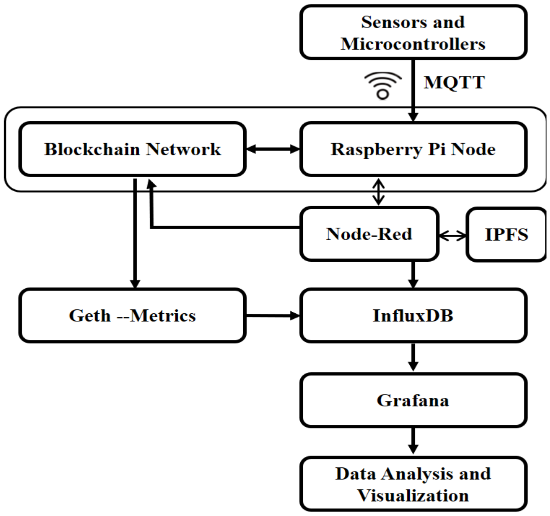


Figure (35): Data flow diagram for BCoT performance evaluation.

With each advancement in blockchain technology and subsequent waves of adoption, meticulous observation and analysis become increasingly crucial. By tracking metrics, one can identify bottlenecks or inefficiencies, determining whether these issues can be resolved or tolerated. Obtaining metrics for Ethereum-based blockchains is an effective method for monitoring and analysing various performance aspects of a blockchain.

The evolution of Blockchain technology is an ongoing process characterised by the introduction of novel features, algorithmic enhancements, and fluctuations in transaction volumes, all of which can significantly impact its computational attributes. In this context, Geth metrics serve as a vital tool for gaining comprehensive insights into these transformations. These metrics enable developers and system administrators to critically evaluate the ramifications of updates, identify performance bottlenecks, and implement informed modifications to optimise system efficiency. Consequently, this data-driven approach facilitates the refinement of Blockchain systems, ultimately leading to an enhanced user experience.

The continuous development of Blockchain technology necessitates a robust framework for monitoring and analysing its performance characteristics. As the technology progresses, incorporating new functionalities, refining algorithms, and adapting to varying transaction loads, it becomes imperative to assess the implications of these changes on the system's computational profile. Geth metrics provide a crucial mechanism for capturing and interpreting these evolving dynamics, offering valuable insights to Blockchain development and management stakeholders. By leveraging these metrics, developers and administrators can effectively gauge the impact of system updates, pinpoint areas of inefficiency, and implement targeted optimisations. This data-driven approach to Blockchain management enhances system performance and improves user experience, fostering wider adoption and utilisation of Blockchain technology across various domains. One of the significant benefits of Geth metrics is their ability to monitor resource usage (e.g., memory and CPU usage), allowing them to pinpoint bottlenecks in performance. Once the reason for a performance bottleneck is identified, the affected components can be optimised, whether it is a software patching and upgrades or hardware or network configuration. Another essential metric in Geth is monitoring network traffic for capacity planning and performance optimisation. This enables the administrator to spot the traffic patterns and accordingly scale resources or use optimisation techniques to eliminate any performance bottlenecks or congestion on the system ahead of time. Moreover, Geth metrics enable benchmarking between different Blockchain systems and help decide which offers the best performance for a particular use case. This will give developers and organisations options and flexibility by allowing them to design, build and operate a ‘bespoke’ custom Blockchain that suits their needs. Even more importantly, Geth metrics contribute to increased performance and a pleasant user experience. For instance, preventing potential problems with user experience – for example, slow response times or congestion in the network – means that administrators can collect, monitor, and react to these metrics before these problems happen. However, monitoring and optimising the performance will become critical as Blockchain technology matures and becomes more widespread. Geth metrics will provide a valuable framework for this task to Ethereum-based Blockchain developers and administrators to keep their systems well-maintained and ready to grow at the pace of the demand.

Geth is the component that exposes the metrics directly to an InfluxDB database—using the --metrics. influxdb flag, along with the URL, username, and password where it should be stored by specifying --metrics. InfluxDB will monitor the node in near real-time. Prometheus-formatted metrics data can be fetched by requesting it at the /debug/metrics/Prometheus URL. Grafana, a monitoring application for collecting and analysing data, offers an out-of-the-box dashboard for monitoring Geth nodes that provides rich insights into the operational aspects of our Ether node. It separates these metrics into system, network and Blockchain metrics. System metrics include overviews of the BCoT node's resource utilisation, which monitor CPU usage, memory consumption, disk input or output, and the amount of network data sent and received. It is a good idea for the system page to validate under what conditions the CPU jumps by looking at the CPU metric; alternatively, it also monitors the number of concurrent Disk I/O reads or writes similarly. In Addition, one can directly observe a two-time series of the memory utilised by Geth, as well as the total memory available to the node and other information. The network section logs the number of peer connections, while one can select and monitor a specific peer. One can then be selective of which peers to prune.

From a programming philosophy perspective, Geth's metrics model is designed to be seamlessly integrated throughout the codebase, akin to the application of software logging. Minimal effort is required to introduce a metric at any point, and the API will expose it. Metrics can and should be updated safely anywhere in the codebase while the system is operational. They are automatically recorded via an API and can be displayed as needed.

Metrics become accessible when the --metrics flag is enabled at start-up, with an HTTP server providing them if --metrics.Address is specified. The default address for metrics is 127.0.0.1:6060/debug/metrics, though custom addresses and ports may be set. The --

metrics.Expensive flag enables more computationally intensive metrics, activated by the following command:

```
sudo geth --datadir "./pidata" --syncmode "full" --port 30305 --http --http.addr
"192.168.1.80" --http.port 8546 --http.api "personal,eth,net,web3,txpool,miner" --
networkid 101020 --nat extip:192.168.1.6 --netrestrict 192.168.1.0/24 --unlock
0xd5e47682bf66a3b34ba04ddda399827c575b7359 --password "./pidata/PWSS.txt" --
allow-insecure-unlock --http.corsdomain '*' --mine --miner.etherbase
"0xd5e47682bf66a3b34ba04ddda399827c575b7359" --metrics --metrics.influxdb --
metrics.influxdb.endpoint "http://192.168.1.80:8086" --metrics.influxdb.username
"admin" --metrics.influxdb.password "Jordan@2020" --bootnodes
enode://cbf4c5e21d15592a9d1ec9b7204cdb4905103aa0ee2b758798c436bbc43f5ccb2de
a2e53a9d9b3ec373ed9df018b6df3a0c2733ebfe58bdd13eaa1f5c40d7762@192.168.1.6:0
?discport=8008 --ws --ws.port 8544 --ws.addr "192.168.1.80" --ws.origins "*" --ws.api
"web3, eth" --metrics --metrics.addr 192.168.1.80 --metrics.port 9090 --
metrics.expensive console
```

As such, Geth metrics are piped into Grafana and displayed as panels with information on every metric of the BCoT's performance. The Grafana dashboard can have multiple panel options, which provide data points that give insight into the health and performance of a Geth node. Grafana is integrated with Geth, enabling real-time monitoring of these values, meaning the Geth nodes can stay in optimum shape, making informed choices with the help of live monitoring.

7.6 Performance Characterization and Validation of BCoT Architecture

Experiments were conducted to assess the real-time capabilities of an architecture designed specifically for the RPi4. The studies examined the average total time, transaction submission latency, and average throughput of a private Ethereum network at different transaction volumes.

The findings, outlined in Table (2), provide a thorough summary of performance features noted across transaction volumes varying from 10 to 1000 transactions. To guarantee a comprehensive assessment, the tests were carried out in two phases, with phase one employing 2,000,000 units of gas and phase two using 10,000 units.

An innovative element of this research is examining gas limit and gas price parameters, which substantially impact user transaction fees. During the initial stage, a gas limit of 4,700,000 units was established with a gas price of 1 GWei, and every transaction used up 10,000 units of gas. The gas limit remained at 4,700,000 units during the next round, but the gas price was increased to 4,700,000 Wei. This change led to higher transaction fees due to the increased gas price, even though the computational resources required for each transaction were reduced.

The experimental findings demonstrated that the interaction between gas price and gas consumption significantly impacts transaction fees and overall throughput. This insight enables users to experience varying charges based on their willingness to pay for expedited transaction processing, which is particularly beneficial for devices with limited resources, such as the Raspberry Pi 4. Moreover, the experiments emphasise how gas-related factors, like gas limit and gas price, are crucial in indicating the system's approach to resource management. Setting a gas limit of 4,700,000 units and a relevant gas price, the research showcased a well-rounded strategy for resource distribution, crucial for upholding system efficiency while handling.

Table (2): Average total time, latency, and throughput for different transaction volumes.

Transactions	**Average Total Time (s)**		**Average Latency (s)**		**Average Throughput (transactions/s)**	
	Round 1	Round 2	Round 1	Round 2	Round 1	Round 2
10	0.3504	0.2813	0.0350	0.0281	28.53	35.68
20	0.6634	0.5532	0.0330	0.0271	30.18	36.76
30	1.0537	0.8060	0.0351	0.0269	28.39	37.40
50	1.7147	1.3272	0.0344	0.0262	29.16	37.64
100	3.5752	2.6280	0.0358	0.0266	28.04	37.91
1000	36.2298	26.9746	0.0362	0.0269	27.81	37.96

Regardless of the different and variable transaction volumes, the experimental average value of the total time to process transactions changed linearly, confirming the architecture's proportional dependence on transaction processing. It is precisely what is expected from an architecture working with transactions since the higher the transaction volume, the higher the total processing time. The average latency per transaction shown in Figure (36) remained relatively stable throughout the experiments, which confirms the consistency of resource use in processing individual transactions. As such, such stability is a positive characteristic of the system's responsiveness during a growing load, which means that the Blockchain network demonstrated a stable level of response to transactions over different loads.

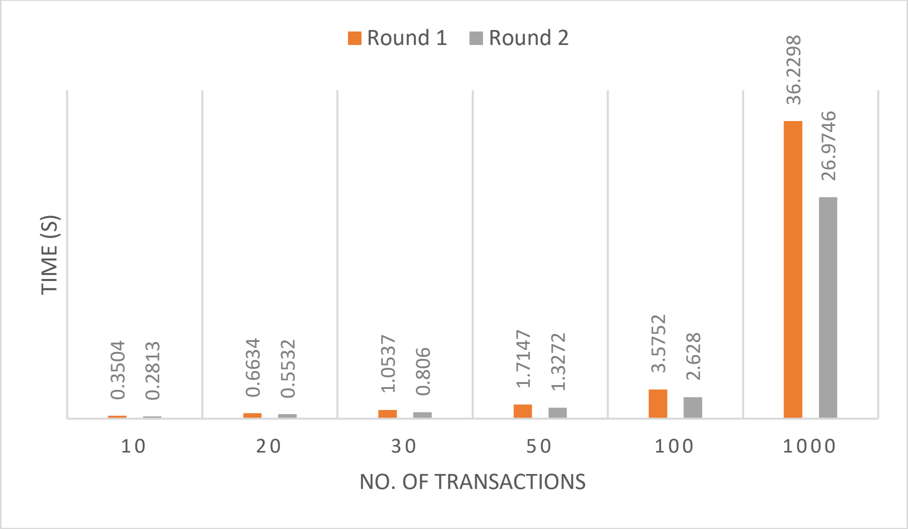


Figure (36): Average total times to process the transactions (s) in the rounds (1,2).

Throughput measures the volume of transactions generated and processed within a given period. The throughput was constant for different numbers of transactions issued, whether round 1 or round 2. The highest number of throughputs is 1000 for an average of 37.96 per second. This constant possibility can imply that the system can handle the load of transactions. The transaction volumes are slightly higher than their previous volumes. This could imply that there is a point that the system works in total efficiency at all of its transaction volumes.

The average metrics table interpretation is a system that maintains stability in latency, takes predictable jumps in total processing time with a more significant number of transactions, and hits an optimum throughput at a high transaction load. These inferences are significant when understanding the system-wide performance characteristics of the Blockchain network while sending transactions of varying frequencies.

A comparison of the transaction cycle for the second round i) throughput ii) average latency Additionally, a comparison of the results of the two rounds reveals that the system was able to support a higher throughput with many transactions, that is, having a peak of 37.96 transactions per second for 1000 transactions. Moreover, it is possible to note how the average latency computed per received transaction decreases with the transaction load growth (i.e., latency proportionally grows with the increase of additional transactions received by the server). Sometimes, the latency has a constant value when the system reaches the peak of the processing load, with the lowest latency computed for 1000 transactions and equal to 0.0269 seconds per received transaction. These results demonstrate the scalability of the system and its ability to cope with large transaction loads with a very acceptable latency, which is a prerequisite for IoT applications that deal with data to be processed in real-time or near-real-time.

Compared with the results in the previous heterogeneous lightweight Blockchain-based marketplace (HLBM) obtained by Guerra et al. (Guerra, et al., 2022), the proposed novel architecture demonstrated better performance in terms of both throughputs and latency, standing at the top of the table of existing solutions.

The HLBM was designed mainly to address the problems of using Blockchain to process requests from constrained resources IoT devices. The proposal bridges a public Blockchain based on transparency and a private Blockchain based on efficiency to establish a secure transaction between IoT devices. Furthermore, Chen et al. tested private Blockchain transaction throughput, latency, and scalability in an experiment regarding private Blockchain technology's performance in IoT applications. The finding indicates that Blockchain technology is essential for various applications (Chen, et al., 2021).

In the proposed novel architecture, the network latency was consistent across the blocks. In addition, the entire traffic is well distributed across all the blocks of transactions. Hence, the network could handle any scale of traffic. Moreover, the network throughput is higher in blocks with more counts of transactions, showing how the system can scale with load. As anticipated, we had little fluctuations in errors and network latency throughout the rounds of experiments. The measurements made in both rounds of performance experiments suggest that Blockchain technology is essential for various applications.

The network parameters with performance are disk space usage, memory usage, and CPU utilisation. The disk performance counter shows how these parameters store and transfer files. The disk reads the data counter, and the disk writes the data counter, indicating the average size of data transferred in reading and writing operations. These two counters also measure the number of read and write operations per second. Watching these two counters helps system administrators see existing trends of disk activity and find the problems and opportunities for improvement. Figure (37) shows the disk read and write operations before and after the transactions and mining process. When Geth begins to start transactions and mining, it will fully load the needed data from the Blockchain database to prepare itself. It attempts to reconnect to the network by logging. Once the transactions and mining process starts, the read and write operations from disk increase dramatically because Geth now actively requests and updates data from the Blockchain database. We can notice that the number of disks write operations is usually more significant than disk read operations as Geth constantly records new data to the Blockchain database while transactions are being processed and blocks are being mined. The figure above shows that disk read and write operations can vary significantly over time. We can see that the size of transactions and blocks can be of enormous difference due to their various sizes. For instance, if there is an abrupt increase in the number of transactions submitted to the network, the disk read and write operations will be increased accordingly.

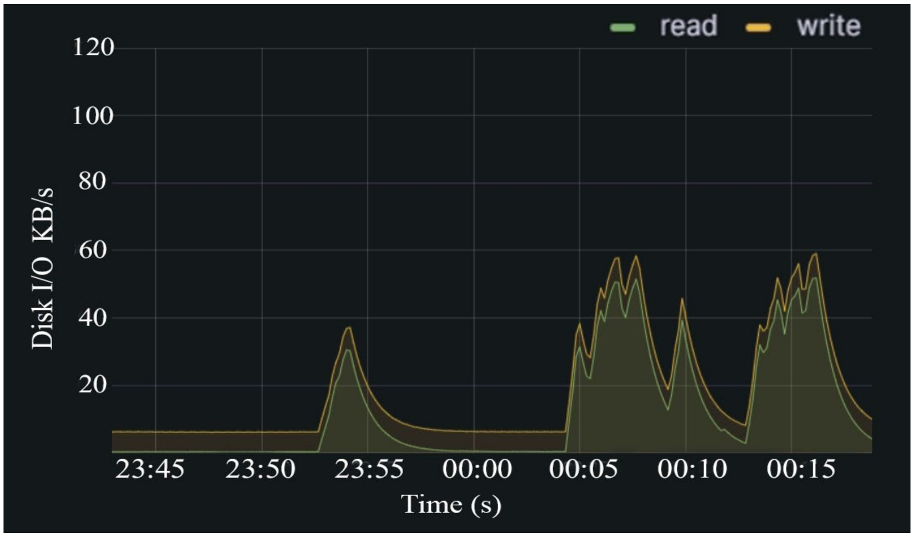


Figure (37): Disk performance monitoring using Grafana.

Figure (38) illustrates that mining RPi4 nodes requires memory usage ranging from 100 MB to 200 MB. Furthermore, memory consumption rises notably when the transaction being processed loads extra data into memory, like the Blockchain database, transaction pool, and account state. Furthermore, memory consumption can fluctuate wildly as the quantity and magnitude of transactions can differ significantly. Geth might also have to bring more data into memory to handle the transactions. The highest amount of memory used is approximately 210 MB, presumably due to Geth handling numerous transactions. Memory usage slightly decreases as Geth completes processing a portion of the transactions. Still, memory usage stays high as Geth handles incoming transactions and upkeeps the Blockchain database.

Figure (38) offers a helpful summary of memory usage following the completed transactions. This data can help address issues with performance and pinpoint opportunities for improvement. For instance, memory usage grows slowly, indicating that Geth consistently brings more data into memory. Furthermore, there were multiple instances of increased memory usage when Geth handled numerous transactions. The memory usage seems to level off eventually, indicating that Geth has achieved a consistent state of handling new transactions and releasing unused memory.

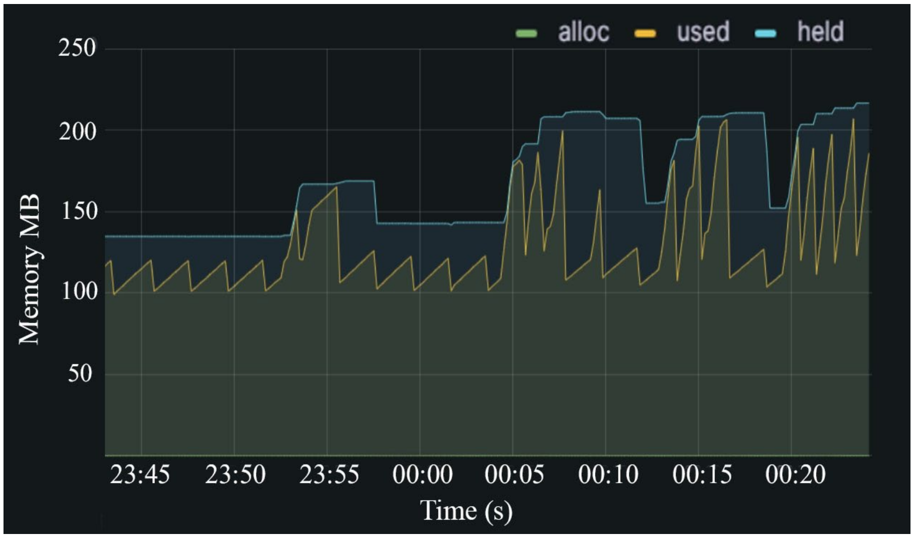


Figure (38): Memory usage using Grafana.

On the other hand, Figure (39) illustrates the CPU utilisation rate of each node. In the RPi4 nodes, the CPU utilisation is approximately below 33%. At the same time, almost all CPUs are consumed during mining on the RPi4. Because the Geth Metrics command calculates the CPU utilisation, it is slowly increasing, and the average CPU time since booting is stable. On a long-term basis, CPU utilisation of RPi4 nodes is stable.

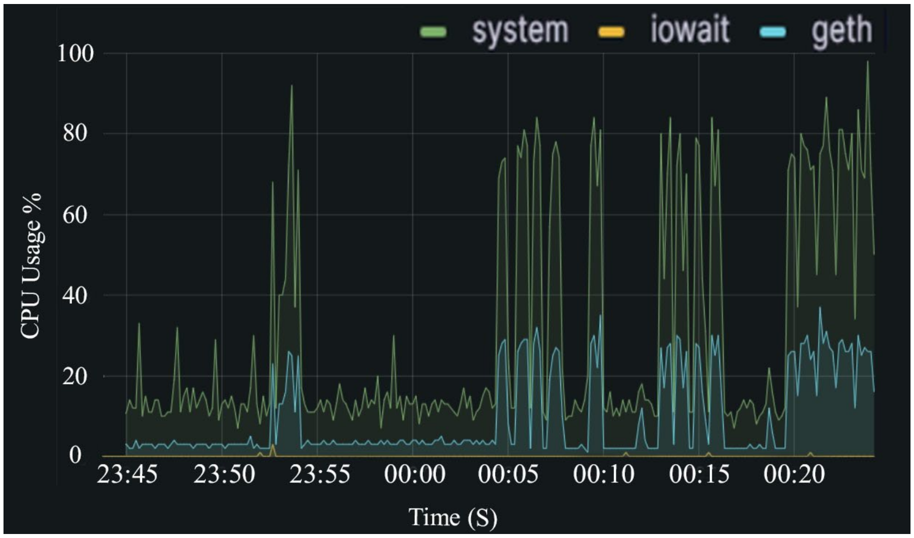


Figure (39): CPU utilisation using Grafana.

Figure (39) also shows that the CPU usage increases significantly in the last time-start after the transaction is submitted, as Geth needs to use more CPU resources to process the transactions, such as inspecting the signatures of the submitted transactions, updating the Blockchain database every time a new block filled up with the transactions is generated, and syncing up with the other nodes on the same network. CPU usage also appears to increase periodically, which is seemingly at the time when Geth is processing many or more complicated transactions repeatedly. The CPU usage seems to return to a stable level after some time, indicating that Geth has reached a steady state of processing new transactions and freeing up any unused CPU resources again. After some time with low CPU usage, the CPU usage seems to increase gradually over the period, indicating that Geth still continuously uses more CPU resources to process the transactions. Several times, when there are too many transactions or somewhat complicated ones to process, we can observe some spikes in CPU usage. The CPU usage returns to a steady level after some time, indicating that Geth has reached a steady state of processing new transactions and freeing up any unused CPU resources again.

The outcomes concerning the performance metrics of latency were benchmarked against the results, which showed an average latency of 9ms compared to 35ms for the solution proposed by Chen et al. (Chen, et al., 2021). The lower latency in the study by Chen et al. was because the proposal was validated using a high-processing device, specifically a laptop, as one of their architecture components. This selection of hardware for validation likely led to faster processing and validation of transactions, hence reducing the latency compared with the proposed solution. Additionally, latency, throughput, CPU usage, memory utilisation and disk I/O results are measured and compared with the HLBM results from Guerra et al., presented in Figure (40). Latency measured for 100 transactions latency is at 6.5(s), whereas in our solution, latency is at 3.5752 (s). However, the proposed novel architecture is more successful in throughput, reaching 35.76 transactions per second, which exceeds the HLBM outturn of 21.6 TPS in throughput. These figures suggest a possible trade-off between latency and throughput achieved by the two solutions.

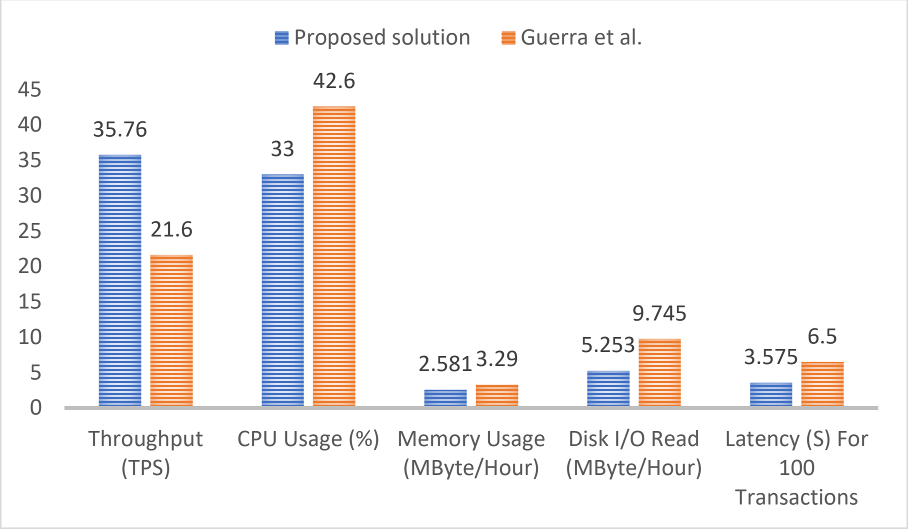


Figure (40): A comparative analysis of the proposed BCoT system with the Guerra et al.

Further analysis of the CPU resource utilisation shows that, on average, the HLBM has higher CPU usage than the memory overhead, which illustrates that HLBM was 11% busy. In comparison, ours was 33%, and this might be because of the different amount and nature of the algorithm computations that might be different in both implementations.

Both solutions have similar memory allocations, but in transactions, HLBM and ours utilised an average of 3290 bytes/hour and 2581 bytes/hour for funds transfer, respectively. This might be because both applications may use almost the same amount of memory in these transactions.

Finally, the disk I/O usage performance shows that the proposed novel architecture read and write was lower than HLBM, and this can be corroborated from the information that disk I/O read statistics is 5253 bytes/hour, which is relatively lower as compared to 9745 bytes/hour in (Guerra, et al., 2022) .

However, it is essential to consider these performance metrics holistically, all taken together, for the entire system of private Ethereum Blockchain works together to deliver the economics of the transactions, on the one hand, and the network performance under load. From a responsibilities and constraints point of view, a system needs to explore the interplay of computational resources, the throughput of data, and the storage required in the Blockchain network to optimise its performance while retaining the integrity and security of the system.

7.7 Enhancing IPFS Efficiency in Dockerized Private Networks: A Performance Evaluation Perspective

A comprehensive evaluation examines how IPFS performs in a Docker container environment, looking at the impact of migrating IPFS within a containerised setting. The latency of writing and reading operations for various file sizes was measured using a test system with three IPFS nodes in Docker containers and an IPFS Cluster peer in Docker. One significant result of the research is that IPFS performed better in Docker with lower latency times than previous studies using IPFS in a stand-alone setup. The efficiency is improved due to the critical factors of the IPFS Cluster replication strategy and the capability to set replica placement using optimal network routes. The studies also emphasise the significance of dynamic resource allocation in maximising the utilisation of hardware resources and, in turn, improving the efficiency of IPFS Clusters. All these experimental assessments offer significant results for implementing IPFS in a decentralised storage setting for a business. The research highlighted the possible use of IPFS in a Docker for a productive and scalable solution that can be accessed remotely online. The authors illustrated the feasibility of storing, managing, accessing, editing, and distributing data via IPFS on Docker, showcasing its suitability for cloud and web applications. The combination of IPFS and Docker enhances the benefits of containerisation, significantly improving the HTTP experience compared to the traditional Web with its easy deployment, seamless scalability, and precise resource isolation.

7.7.1 Background and Problem Statement

IPFS is one of the latest innovations in P2P file-sharing technology that cuts directly at the heart of client-server technologies such as HTTP (Zheng, et al., 2018). IPFS combines DHT, MerkleDag data structures, and the BitSwap protocol to enable direct P2P file exchange. Using a DHT, IPFS allows peers to discover content across the network and efficiently retrieve it using content identifiers. MerkleDag data structures allow files and directories to be unambiguously addressed, connected, and named (Huang, et al., 2020). Tracing back to BitTorrent, BitSwap coordinates data transfer among peers, optimising decentralised data retrieval. IPFS promises to offer uncensored file sharing. It is virtually impossible to take down shared content using IPFS since each piece has an allocated IPFS reference, immutable and permanently linked to the data. This makes it a valuable tool for archiving. In addition, the system ensures efficient distribution of the content and can avoid redundancy (Pandey, et al., 2023) (Xu, et al., 2018) (Bhadula, et al., 2023) (Shin, et al., 2023).

IPFS can also operate fully offline with no internet connectivity, acting as a cache that can be accessed despite these limitations. It represents the future for next-generation file-sharing systems, offering improved resilience, efficiency, and accessibility.

This research work investigates the performance of IPFS in private networks. This study aims to compare the performance of IPFS in Private networks and identify the factors affecting its performance when used in Local Area Networks. A private network was created using a technology called "Docker-Cluster". All IPFS Cluster nodes formed the private libp2p owned by the cluster and maintained the IPFS list of CIDs and the metadata about which IPFS node pinning that content. When one of the nodes of the IPFS Cluster adds a new file, it informs the Cluster about that operation. Cluster nodes will coordinate the replication of that content among three IPFS nodes. The creator may configure the IPFS Cluster to keep the content in some specific locations, or it may be configured to pin the content across all three IPFS nods based on the storage space. That means one can determine where content should be replicated and pin it on nodes with excess storage.

Then, several files of various sizes will be created and separated between these Docker containers. The operation latency for each operation will be monitored. The question is how IPFS performs in writing or reading data to or from an IPFS-Cluster private network built using the Docker technology and which affects the performance of IPFS writing and reading in private Docker networks.

The primary objective is to propose an application of using the IPFS-Docker network for file-sharing systems as an alternative to client-server-based file-sharing systems. It will establish the score for developing a file-sharing application on top of IPFS-Docker for private networks. Also, it motivates designers of IPFS to attempt to use new methods in the file system to achieve better performance. In addition, another research aim is to investigate the impact of using private computing networks on the performance of file-sharing systems. It focuses on the potential of re-engineering file-sharing systems to take full benefit of private networks and achieve optimal performance.

Several research articles and studies have also investigated the performance of IPFS storage, indicating its uniqueness and limitations. For example, Shen et al. (Shen, et al., 2019) investigated the performance of IPFS on the client side to understand how file size, concurrency, node, and network topology affect throughput, latency, and scalability. The authors used a custom-built IPF client to run their experiments on an IPFS cluster with a variety of node configurations, which helped to understand the performance of the decentralised storage on different scenarios and workloads. These findings significantly impact the optimisation of IPFS reading and writing and the deployment of IPFS into applications. The case study results revealed that increasing the data sizes would degrade IPFS performance significantly, even in the case of slow networking – meaning fetching data would become slower. Further measurements of the time-based performance of the IO operations showed two significant bottlenecks for reading data from remote nodes: the resolving process and the downloading of IPFS data blocks. The academic storage cluster (ASC), a decentralised storage system based on IPFS, specifically designed as a modern peer-to-peer infrastructure for the academic community (Tottleben, et al., 2021), was studied. The ASC aims to provide a secure, reliable, scalable storage and sharing system for research data, papers, and other academic artefacts. The paper presents the preliminary results of the pilot deployment of the decentralised system and its feasibility and benefits for the academic community. The study showed that ASC can show proof of concept that provides a secure and decentralised alternative to traditional centralised storage. The decentralised nature of the system enables the teacher to protect students' privacy and maintain control of their work. It also showed that an ASC deployment can positively impact the academic community's work and collaborations. This is an ongoing study by the research community for decentralised academic and research data storage. Lajam and Helmi (Lajam & Helmy., 2021) investigated and evaluated the performance of IPFS in private networks and the effects of private network characteristics, such as network size, node degree and latency, on various performance metrics, including data retrieval time, bandwidth usage and node storage usage. The authors presented the results of simulated and empirical studies on the performance of IPFS in private networks. The study demonstrated that factors such as network topology, node connectivity, and the number of data block copies in the cluster influenced the performance of IPFS in private networks. The performance of IPFS in private networks can be improved in several ways, including reducing network latencies using methods similar to techniques for traditional client-server read and write optimisation. Ahmad et al. (Ahmad, et al., 2023) investigated the performance of reading data in the IPFS clusters. They showed that the size of the cluster (the number of connected nodes) does not affect performance, but the replication factor (the number of copies of data blocks in the clusters) does. An IPFS cluster is a distributed set of nodes which acts as a single distributed storage unit in the network. It is different from the IPFS private network, where each node has independent files in the network.

7.7.2 Experimental Testbed

The experiments were conducted on the host machine with a 4-core 2.5 GHz i5 Intel processor, 12 GB RAM, and an SSD disk. As the host machine, windows 11 was installed using Windows 11 development tools. Using Docker Desktop, an IPFS cluster composed of three IPFS node nodes was installed into three containers. Figure (41) shows the architecture diagram of an IPFS cluster. Meanwhile, a Docker container is to host the FTP node with the VSFTP technology. With this IPFS cluster architecture, the following examines the configuration of the IPFS cluster and the impact on data storage and retrieval performance in terms of efficiency. By assigning a different role to each node of the IPFS cluster installed in a Docker container and exploring the details of sharing data in closed-network scenarios, a typical architecture diagram of an IPFS cluster can be presented, showing that node (n) can be different roles such as redistributing blocks of data, storing peers list or data to perform tasks such as searching, and verifying the integrity of data. Hence, the detailed impact on private network IPFS could be explored further. The goal is to build a system of playbooks to perform tasks on end-point device clients that can auto-detect local applications and have their local data uploaded to an offsite IPFS network for more scalable sharing.

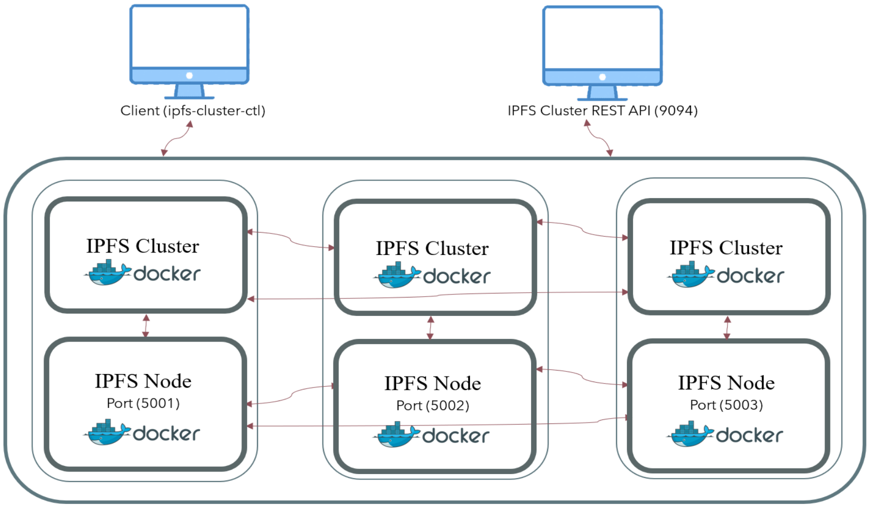


Figure (41): The architecture of the IPFS cluster.

This Docker compose file defines several services for IPFS nodes (ipfs0, ipfs1, ipfs2) and IPFS Cluster peers (cluster0, cluster1, cluster2). All these services are containerised, giving each process an entirely isolated execution environment. Each IPFS node (ipfs0, ipfs1, ipfs2) has exposed ports for IPFS, API and gateway. Ports are used for both intra and inter-service communications. IPFS nodes will be required for data addition to or retrieval from IPFS. IPFS ports (12700, 12701 and 12702) are used for communication with IPFS nodes. Exposed gateway ports (8080, 8082 and 8083) with 5001, 5002, and 5003 are used for reading operations, while ports 5001, 5002, and 5003 can be used for writing operations. This includes IPFS content addition (writing content to IPFS) and reading (fetching files and performing content addressing).

Each IPFS Cluster peer (cluster0, cluster1, cluster2) depends on a corresponding IPFS node with which to work. This dependency is crucial because it enables communication between

Cluster peers with their corresponding IPFS nodes for data management. IPFS Cluster peers enabled read operations by coordinated data retrieval from the IPFS node. The Cluster peer can handle client requests for data. The peer can retrieve the requested data from the IPFS node (CLUSTER_IPFSHTTP_NODEMULTIADDRESS) and serve it to the client via Cluster REST API (9094). The operation for this case involved a query made to the IPFS node for the requested data and then returned the content to the client. IPFS Cluster peers could also write operations by coordinating content addition tasks across the IPFS nodes. The peer can access new content to add to Cluster.

The peer will distribute the added content to the associated IPFS nodes (CLUSTER_IPFSHTTP_NODEMULTIADDRESS). The IPFS nodes will then upload the content to the IPFS network. Clients mostly used the Cluster REST API (on port 9094), which provides endpoints for different operations, including putting and getting data, adding/deleting/editing peers, and monitoring the cluster's status. The ipfs-cluster-ctl command-line tool is provided to interact with the cluster, and the operations include managing peers, querying data, and monitoring the cluster's performance. One of the advantages of using IPFS in Docker with a cluster setup is its ability to provide high availability, load balancing, redundancy, fault tolerance and horizontal scalability. IPFS Cluster works to coordinate a collection of nodes to provide decentralised, distributed access to content requested by parties.

The data for the cluster can exist on multiple nodes, and at a lower level, these data points are asymmetrically connected through an overlay-style network. In a cluster, nodes can play different roles. A tracker node keeps track of where content is and forwards requests to the storage nodes that know the address of the specified content. These storage nodes or pin nodes essentially store and replicate data for redundancy and fault tolerance. Moreover, a rest API node is the one that exposes the cluster's API to external clients for management and monitoring capability.

7.7.3 Experimental Material and Design

Data files (the materials of experiments) were transferred between nodes in the private network, and writing and reading operations were performed on those files. Two groups of files, one relatively small and the other large, were included in the experiment. The small files are 1 KB, 4 KB, 16 KB, 64 KB and 256 KB, while the large files are 1 MB, 4 MB, 16 MB and 64 MB. These sizes of files were chosen based on the work of Lajam and Helmy. The IPFS splits the files into 1 MB blocks. Therefore, the larger files require more processing time. The files were created manually in those sizes. The content of these files was simply arbitrary alphabetical characters equally filled in the created files that the experimenter had created.

Measurements were taken to and from the network via file-writing (into IPFS) and file-reading (from IPFS) operations. In other words, these measurements were performed on the operations of reading a file and writing a file using IPFS. The command ADD written in IPFS conducted the file-writing operation. Resetting the IPFS network to keep the local state, a file is added to local IPFS, and the local version of the file, once added, is available to members of the IPFS network, specifically other peers in that network. The GET command conducts the file-reading operation, downloading a file from the IPFS network from one or more nodes holding the file. Downloading a file adds it to the local IPFS repository for that node that requested it. It becomes available to provide to other IPFS network members, increasing the number of contributors (also known as file senders) as the number of owners of the file increases. In this experiment, there are two steps: resetting to keep the local IPFS network state and either node one or node 2 accepting the operation (read or write file) from the other.

Latency was measured for all operations as the time elapsed from the beginning of the operation attempted by the user until its end, i.e., operation completion time, and this time includes CPU time, I/O waiting time, and network delay. For writing operations and reading operations in IPFS, in the writing operation experiment, the first operation involved invoking the content to IPFS via writing it to IPFS. In this process, the 3 API nodes (5001, 5002 and 5003) were used, and the content was added to the IPFS network via command-line tools like ‘ipfs add’. In the reading operation experiment, a reading method from IPFS data was first selected (via gateway ports, for example), and afterwards, the added content was retrieved. Since the reading method was via the gateway port for IPFS, the ‘ipfs cat’ was used afterwards to retrieve the content to be retrieved according to the command line tools like ipfs add. Test reading from the IPFS cluster via Cluster REST API was performed

(9094). All operations were invoked for ten files and then measured and recorded afterwards.

7.7.4 Comparative Analysis of Latency and Resource Utilisation in IPFS vs. FTP Systems within Docker Environments

Figures (42) and (43) illustrate the detailed comparison of the latency in writing operations between IPFS and FTP for small and large files. The latency measurements for writing files to the local IPFS-Docker network and the FTP container show distinct differences between the file storage systems. The latency for IPFS is significantly greater in milliseconds compared to FTP. The reason for this is the extra tasks carried out during the IPFS writing process, like breaking big files into segments and creating distinct CIDs for each segment. On the other hand, the FTP writing operation is a straightforward copying process. IPFS latencies show minor differences for small files comprising one block but are noticeable for large files divided into several blocks. This is because more I/O disk operations are needed to manage the increased number of blocks in larger files. This indicates that writing one large rather than multiple small files in the IPFS system is more effective. Examining the writing efficiency of individual file systems, the findings suggest that writing big files to IPFS is not as effective as writing a single big file. This is probably caused by the elevated I/O disk operations needed to manage the numerous blocks of a sizable file in IPFS.

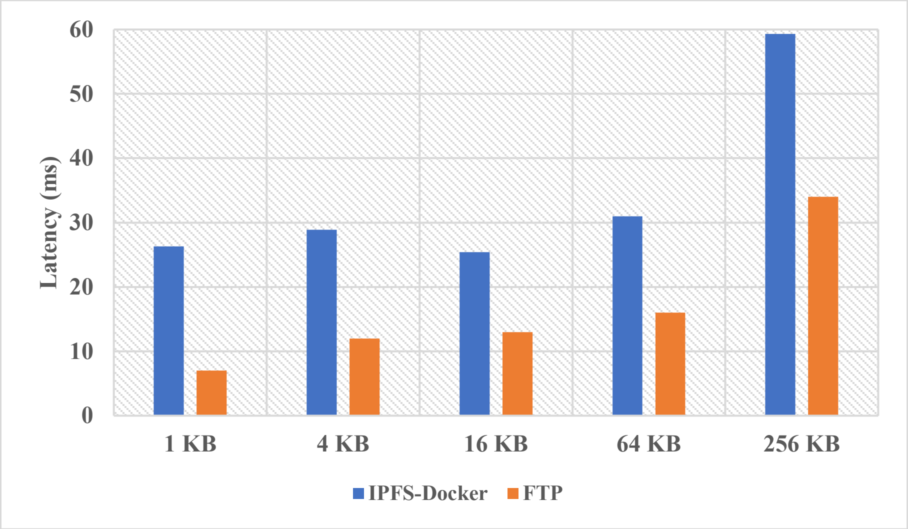


Figure (42): The latency for the Docker cluster and FTP writing operations for the small-size files.

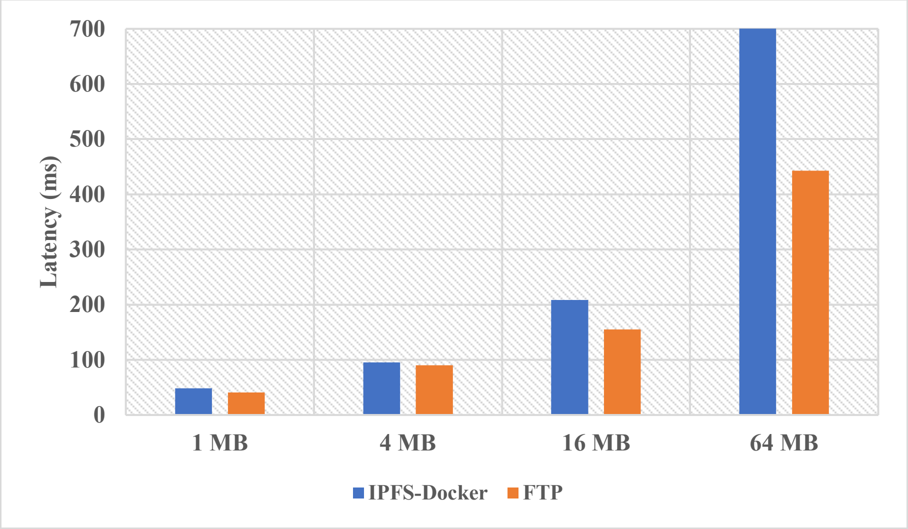


Figure (43): The latency for Docker cluster and FTP writing operations for large files.

Figures (44) and (45) represent the reading operation delay latency to measure the improvement of reading efficiency. The latency between IPFS and FTP is small for small and large files.

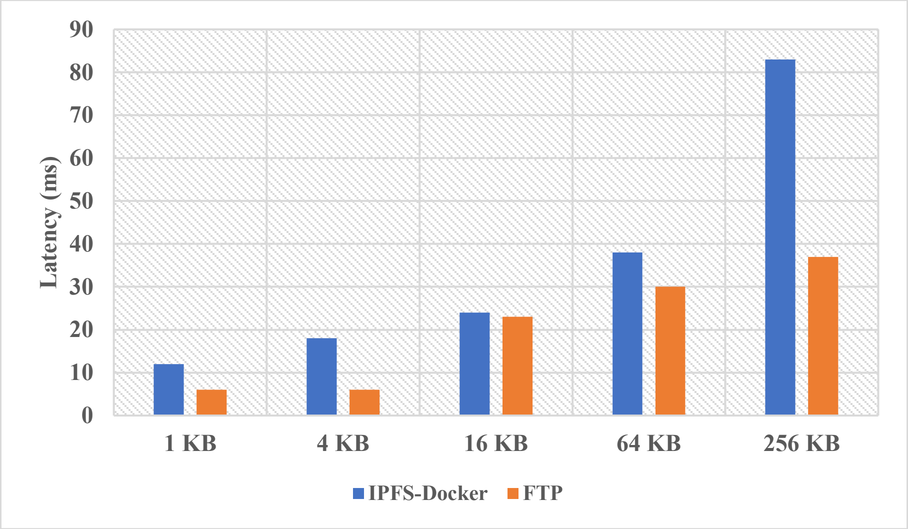


Figure (44): The latency for the Docker cluster and FTP reading operations for the small-size files.

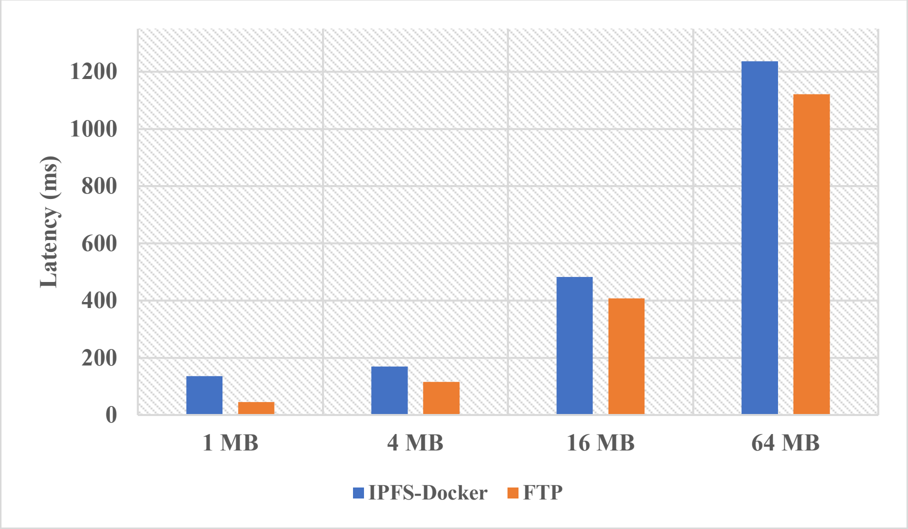


Figure (45): The latency for Docker cluster and FTP reading operations for the large-size files.

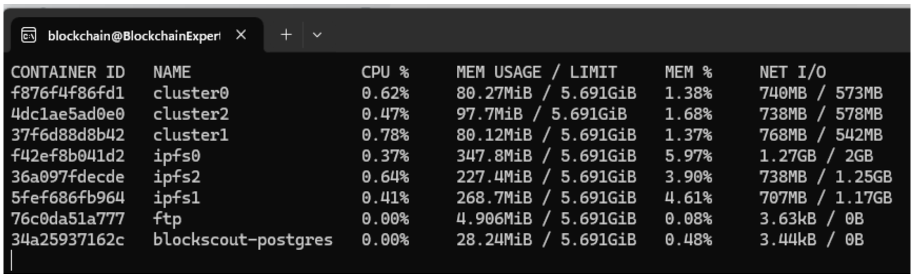
The latency dynamics are different again for a clustered IPFS setup inside Docker. In this case, the broadcast nature of BitSwap itself is perhaps not directly relevant (since data exchanges start and end at replication-management nodes, by necessity). However, nodes in the cluster still exchange data with BitSwap. The latency here ultimately depends on the cluster's replication strategy. The cluster will coordinate handling copies across multiple nodes for any new file being added to the system. This coordination means that individual nodes will be less likely to receive redundant data, potentially improving latency in this setup.

The existence of specialised gateway ports and a Cluster REST API function as entry points for retrieving data, with their effect on latency being more independent of the cluster's node count. Instead, the speed of data copying and distribution among the cluster significantly impacts latency. By having the cluster handle replication, the chance of receiving duplicate data packets is significantly decreased, which could lead to faster response times compared to situations where replication is not utilised. Other factors to consider are the cluster's total workload, which impacts latency while managing different requests and replication jobs, and the connection speed between Docker containers and the main machine, as effective network communication is crucial for latency performance. The distributed IPFS cluster architecture of IPFS Cluster improves data availability, redundancy, and fault tolerance. The cluster comprises multiple coordinated IPFS nodes working together to synchronise data and uphold a unified data replication system instead of just one IPFS node.

The significance of the cluster's replication and data distribution efficiency outweighs the number of nodes in determining latency. When a new file is uploaded to the IPFS Cluster, the cluster coordinates the duplication of the file among various nodes. The cluster's distribution of file chunks reduces redundant data reception by individual nodes through coordinated replication. The primary way the cluster lessens redundant data retrieval is through its replication strategy. Through the innovative distribution of file chunks across various nodes, the cluster prevents nodes from getting duplicate data while handling content requests. This differs from the usual IPFS broadcast model, where duplicated data is more likely to be transferred among nodes. Moreover, dedicated gateway ports and a Cluster REST API offer access points for data retrieval, helping minimise node numbers' impact on latency. The importance of the cluster's replication and data distribution efficiency in influencing latency outweighs the impact of the number of nodes (Kim, et al., 2024).

Docker is well-suited for deploying IPFS nodes. By utilising Docker containers, developers can efficiently operate IPFS in segregated environments. This method enables them to benefit from Docker's capabilities in managing resources. Fundamentally, Docker simplifies the task of operating IPFS nodes while allowing precise management of resource distribution. By imposing restrictions on the memory and CPU utilisation of IPFS containers, individuals can guarantee that IPFS nodes do not utilise excessive resources, as illustrated in Figure (46), avoiding possible declines in performance or depletion of resources on the host system. This is especially crucial in operating several IPFS nodes, as it enables better distribution and use of resources.

On the other hand, it is also possible to run IPFS Docker on top of Kubernetes, a powerful container orchestration engine. Kubernetes can be programmed to dynamically manage resource allocation to instances based on real-time demands, automatically scaling up or down the nodes as needed. This capability ensures that the IPFS cluster is continually optimised for both performance and resource utilisation, ensuring that the workload is distributed across all available nodes and that no single node will become a bottleneck. This combination of IPFS Docker and Kubernetes offers a robust and scalable solution for deploying IPFS-based applications in a containerised environment. (Sivasankari & Sathyamithran, 2022).



```
CONTAINER ID   NAME                 CPU %     MEM USAGE / LIMIT     MEM %     NET I/O
f876f4f86fd1   cluster0             0.62%     80.27MiB / 5.691GiB   1.38%     740MB / 573MB
4dc1ae5ad0e0   cluster2             0.47%     97.7MiB / 5.691GiB    1.68%     738MB / 578MB
37f6d88d8b42   cluster1             0.78%     80.12MiB / 5.691GiB   1.37%     768MB / 542MB
f42ef8b041d2   ipfs0                0.37%     347.8MiB / 5.691GiB   5.97%     1.27GB / 2GB
36a097fdecde   ipfs2                0.64%     227.4MiB / 5.691GiB   3.90%     738MB / 1.25GB
5fef686fb964   ipfs1                0.41%     268.7MiB / 5.691GiB   4.61%     707MB / 1.17GB
76c0da51a777   ftp                  0.00%     4.906MiB / 5.691GiB   0.08%     3.63kB / 0B
34a25937162c   blockscout-postgres  0.00%     28.24MiB / 5.691GiB   0.48%     3.44kB / 0B
```

Figure (46): The Docker stats command returns a live data stream for running containers.

The investigation of resource usage in the IPFS Cluster showed a highly nuanced distribution of user and kernel CPU and memory, which was explained by the different operational requirements of IPFS nodes and cluster containers deployed at various levels. The systematic review and empirical studies helped to further identify the dynamic interaction between resource allocation mechanisms and their effect on Docker-Cluster environments' performance, usability, and scalability (Ahmad, et al., 2023).

The CPU usage on ipfs0, ipfs1, and ipfs2 remains steady at 1%, indicating minimal processing is required. Upon further investigation of memory usage, it was discovered that ipfs0, ipfs1, and ipfs2 had likely consumed significant amounts of their available memory. More precisely, ipfs0 uses roughly 6% of its 5.691GB memory, ipfs1 utilises close to 4.7%, and ipfs2 consumes about 4%. The reason for this memory usage is linked to the tasks related to managing data performed by these nodes, such as data replication, hash calculations, and block administration. Low CPU utilisation compared to high memory usage indicates that memory resources will likely impact system performance more than CPU capacity. These patterns are common in distributed storage systems such as IPFS, where nodes manage metadata and store data blocks. The containers labelled cluster nodes (cluster0, cluster1, cluster2) also show low CPU and memory utilisation levels. The minimal usage indicates that these cluster containers, likely serving as IPFS Cluster peers, perform more effectively than other experiment-related elements. These containers mainly handle metadata and enable node communication, which requires fewer computational resources. Cluster containers are significant in managing cluster operations by effectively controlling resource usage, overseeing coordination, managing replication strategies, and upholding cluster health. This description of how resources are used highlights how effectively the IPFS Cluster's design distributes computational work based on the needs of its components.

An essential advantage of utilising Docker containers for IPFS Clusters is the capability to assign resources dynamically. This implies that the CPU, memory, and storage resources can be modified dynamically according to the cluster's present requirements. This vital allocation is essential for maximising the efficiency of resource utilisation. The overall performance of the IPFS Cluster is improved by automatically adjusting resources based on demand. This improvement guarantees that the cluster is adequately equipped to function efficiently without expending resources unnecessarily on unnecessary tasks. IPFS Clusters can dynamically adapt resource allocations by utilising container orchestration tools like Kubernetes and Docker Swarm to respond to changing workloads and operational requirements. This flexibility guarantees that IPFS nodes and cluster containers receive the necessary computing resources to effectively perform their duties, preventing possible obstructions and improving scalability. Additionally, the cluster can distribute computational resources more efficiently by setting resource limits and quotas and strategically deploying containers according to their resource profiles. This distribution enhances the use of hardware resources and improves the stability and reliability of the IPFS Cluster by avoiding resource conflicts and ensuring fair resource allocation for containers. To sum up, analysing how resources are used in IPFS Clusters shows a complex distribution of computational resources corresponding to the specific needs of IPFS nodes and cluster containers. Utilising dynamic resource allocation mechanisms in Docker-Cluster environments enhances efficiency and scalability, highlighting the significance of adaptive resource management for maintaining performance and reliability in distributed storage systems (Kumar, et al., 2023).

Further, Docker's resource management features can be utilised to set appropriate memory limits on IPFS containers, preventing performance problems. Optimising the cluster's replication strategy and preparing data for distribution will help avoid the need for additional memory on each node. Container orchestration tools such as Kubernetes can dynamically allocate resources to IPFS nodes by ensuring they have the memory required to perform their work.

7.7.5 System Analysis and Validation

Figure (47) and Figure (48) show latency measurements for writing files to the FTP and local IPFS repository containers named ips0 and running on default port 5001, respectively. These graphs illustrate the write operation latency of IPFS for both small and large files in the IPFS-Cluster implementation and compare it to findings from Lajam and Helmi, who reported lower latency in the current Docker implementation for write operations to IPFS.

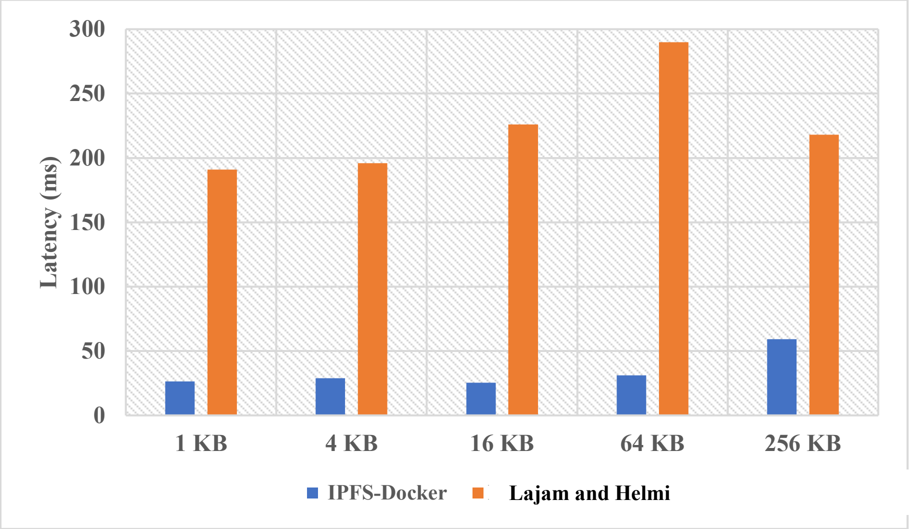


Figure (47): Latency of IPFS writing operations of small-size files in ms.

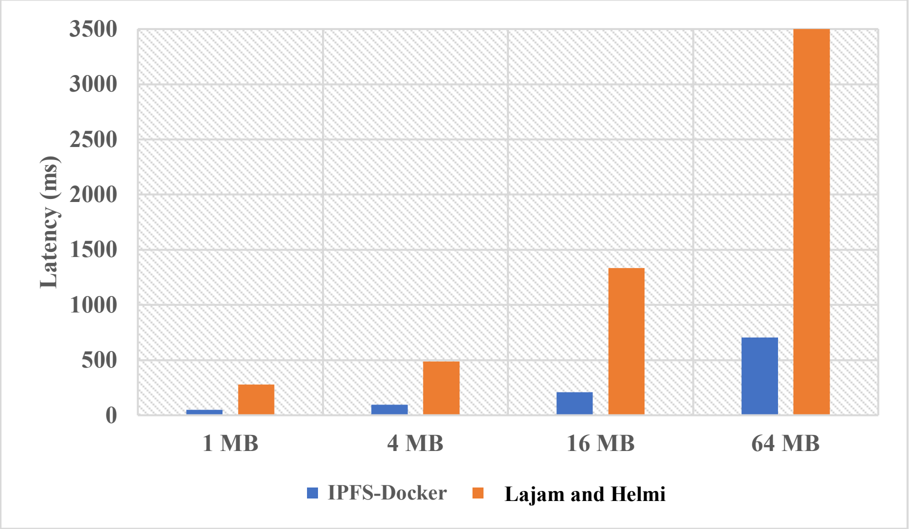


Figure (48): Latency of IPFS for writing operations of large-size files in ms.

Additionally, significant variations in latency were noticed between the two setups, Lajam and Helmi (Lajam & Helmy., 2021), and the current solution, as the efficiency of IPFS in virtual machines and Docker containers can be impacted by various essential factors.

Resources in VMs are distributed at the level of the virtual machine, ensuring a higher degree of performance assurance for the IPFS instance. Nevertheless, VMs experience increased overhead because of an extra layer of abstraction from the virtual operating system, affecting both start-up times and efficiency overall. On the other hand, Docker containers use the same kernel as the host system, resulting in a more lightweight and quicker start-up. However, resource distribution may vary based on the host's workload. Storage and network performance are also necessary, as Docker containers can gain advantages from the host's direct connection to physical storage and network resources. Moreover, the particular IPFS task, including the data size and how it is accessed, can significantly impact performance in VM and Docker settings. Although Docker containers have benefits in terms of start-up time, isolation, and portability, the performance of IPFS deployments dramatically depends on the host system's configuration. (Routray & Ganiga., 2021).

However, the latency tests for saving the files to the FTP and the local IPFS storage units were carried out using gateway ports ipfs1 (port:5002) and Cluster REST API (port:9094). When a new file is uploaded to an IPFS Cluster node, the cluster ensures the content is replicated on all three IPFS nodes. Figures (49) and (50) display the latency for the reading operations, respectively. The latency discrepancy in the IPFS Docker varied significantly for both small and large files in the two scenarios. Nevertheless, the response times for the IPFS tasks in the Docker setup were reduced.

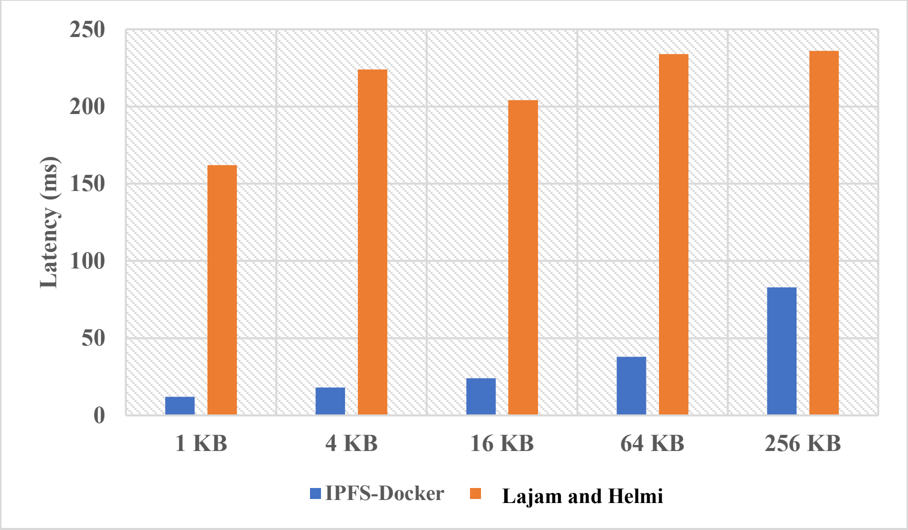


Figure (49): The latency for IPFS reading operations of small-size files in ms

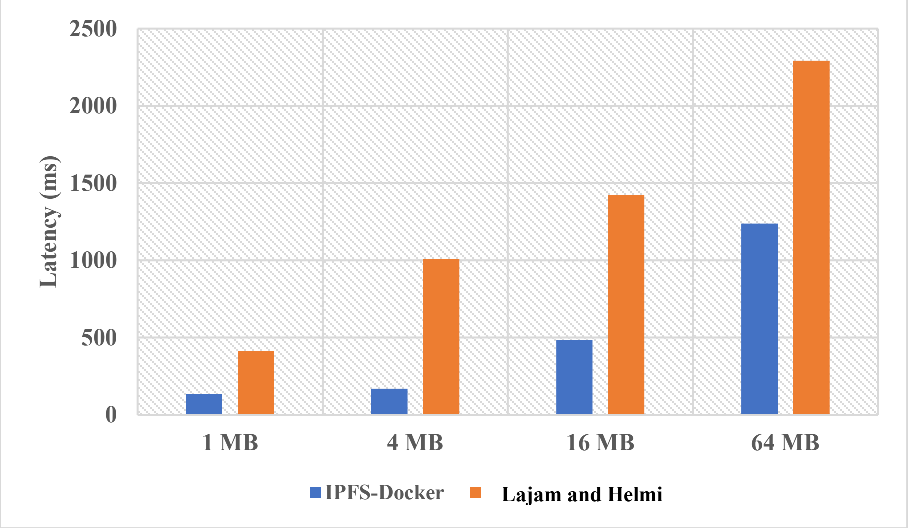


Figure (50): The latency for IPFS reading operations of large-size files.

7.8 Chapter Summary

The proposed novel BCoT architecture was set up and tested, showing promising outcomes demonstrating its technical feasibility and appropriateness. The BCoT architecture was deployed successfully on three RPi4 nodes and operated continuously without significant errors or unusual behaviour, proving its stability, reliability, and suitability for specific IoT applications. Various performance metrics were assessed at various nodes, unveiling significant distinctions. As anticipated, the device with lower CPU speed and RAM produced more moderate metrics than the more powerful RPi4 nodes.

Nevertheless, the less efficient device still met the needs of the Blockchain network, showing that budget-friendly, energy-efficient devices are suitable for the architecture. A positive discovery is that the Blockchain has almost limitless disk space needs. In the most extreme situation, if the RPi4 device consistently used 20 KB of disk space per hour, it would still take many years to fill up 1 GB of storage.

The disk performance indicates that the storage needs of the BCoT architecture are minimal, even for devices with limited resources. This is a significant benefit, as it enables the implementation the BCoT architecture in regions with restricted or sporadic network infrastructure. The assessment showed that the nodes have plenty of resources, with more than 75% of CPU time and less than 6% of RAM dedicated to Blockchain tasks, which is a crucial finding. The excess computational and memory resources allow the nodes to take on extra responsibilities like data acquisition without impacting the Blockchain's efficiency. This adaptability is essential, enabling IoT devices to function as Blockchain nodes and data collection endpoints, simplifying the system architecture.

The testing and assessment outcomes show that the suggested BCoT architecture is technically feasible, scalable, and appropriate. This solution is well-suited for real-world IoT applications and uses cases due to its low-performance requirements and ability to utilise nodes for extra tasks. The BCoT architecture could see enhancements by adding more Blockchain nodes to simulate real-life situations. Several brokers can function as nodes on the Ethereum network in various locations. Additional innovative technologies, like AI, could be integrated into the system to boost its effectiveness and performance through enhancing its predictive and decision-making skills.

Furthermore, this study delves into the performance of IPFS within Docker-Cluster containers, shedding light on its promising potential and acknowledging existing challenges. Despite IPFS's advantages in distributed file systems, such as resilience against single points of failure, its performance limitations have been a concern. This research particularly examines the feasibility of deploying IPFS in private networks within organisations, revealing potential hurdles due to performance compromises. By comparing IPFS performance in Docker-Cluster containers to prior studies, the research underscores a notable reduction in latency attributed to Docker's lightweight architecture and efficient resource utilisation. The experiment underscores the multifaceted nature of IPFS performance, which is affected by variables like file size, replication strategies, and resource allocation. Furthermore, the integration of IPFS with Docker-Cluster demonstrates its suitability for containerised environments, offering scalability and seamless integration with container orchestration platforms like Kubernetes. The study advances the understanding of IPFS performance dynamics and underscores the necessity of adapting distributed storage systems to modern infrastructure for enhanced performance and reliability. In future work, exploring a broader range of file and block sizes, conducting repeated operations for more precise data, and simulating a more realistic virtual environment with increased node numbers could further enrich the findings.

In the next chapter 8: Conclusion and Future Work, Finally, Chapter 8 will present the summary of the significant findings and potential future research directions. The journey ends with a conclusion, where the results are summarised, and their implications for practice and theory are discussed. Limitations of the study are also pointed out, and recommendations for further investigation are made. This is the end of the thesis work. The thesis has provided answers to IoT and Blockchain integration and has given insights that can be transformed into solutions to enhance the performance of healthcare and laboratory management. The road to this point has not been easy. However, it has been a remarkable journey, and the impact of the research could be significant.

Chapter 8

Conclusion and Future Work

8.1 Introduction

The proposed BCoT architecture presented in this thesis successfully demonstrated significant advancements in improving scalability, efficiency, and security within IoT environments. Performance testing showed that the architecture achieved reduced latency and enhanced throughput, making it a viable solution for real-time data management in industries such as healthcare. The novel integration of Blockchain, IoT, and edge computing enabled a robust system that facilitates secure, decentralised data transactions while ensuring the reliability of IoT networks.

However, the research also highlighted several limitations that warrant further investigation. The scalability of the Proof of Authority (PoA) mechanism, though improved, still needs to improve in handling massive transactions under extreme conditions. Additionally, resource constraints in edge devices remain a concern when integrating complex AI and Blockchain functions. Future research should focus on optimising the PoA mechanism and exploring hybrid solutions to accommodate larger-scale deployments. Moreover, advanced security protocols should be developed to counteract potential vulnerabilities, particularly in IoT applications involving sensitive data. Integrating AI-driven decentralised analytics presents another promising area for future work, enabling the system to improve decision-making capabilities and predict critical scenarios in real time.

8.2 Conclusion

The first objective of this thesis was to conduct a comprehensive literature review on the BCoT to critically evaluate the current state of integration between Blockchain and IoT technologies.

The literature review in Chapter 2 gives a detailed picture of DLT and Blockchain Technology. These are some of the key aspects of Blockchain Technology; besides, this chapter provides the reader with an overview of the topic, serves as a base for the study, and indicates the existing studies in this field.

Key aspects:

- DLT is a secure, decentralised system for recording and sharing data across a distributed network. This technology eliminates the need for a central authority by using consensus mechanisms to validate and synchronise data across multiple nodes.
- Blockchain, as a specific type of DLT, is explored in detail. The chapter distinguishes between permissioned and permissionless Blockchain networks. Permissionless networks, like Bitcoin, allow anyone to participate, while permissioned networks restrict access to authorised participants.
- Various consensus mechanisms are discussed, including Proof of Work (PoW) and Proof of Stake (PoS). These mechanisms ensure agreement on the ledger's state across the network.
- The review covers significant Blockchain platforms, focusing on Ethereum due to its smart contract capabilities. Other platforms like IOTA and Hyperledger Fabric are also examined, highlighting their unique features and use cases.
- The chapter focuses on integrating Blockchain with IoT and CPS and introduces the concept of BCoT, a promising convergence of IoT, Big Data, and Blockchain technologies. This integration addresses the limitations of traditional client-server models in IoT applications, paving the way for a more efficient and secure future.
- Key challenges in Blockchain technology are identified, particularly scalability and performance issues. The chapter discusses the inspiring ongoing efforts to enhance scalability, throughput, and latency in BCoT systems, offering hope for a more efficient and scalable future.
- The review also explores Blockchain applications in education, demonstrating the technology's potential beyond CPL use cases.

By covering these topics, the chapter establishes a solid foundation for understanding the technological context of the thesis. It highlights the transformative potential of Blockchain and DLT across various sectors while acknowledging the challenges that must be addressed for wider adoption and implementation.

The second objective of the thesis was to analyse the application of Blockchain technologies within BCoT frameworks, examining their inherent limitations and challenges to identify areas for potential improvement and innovation.

Chapter 2 of the thesis also comprehensively reviews the integration of Blockchain Technology and IoT, exploring their evolution and applications1. It critically examines the limitations and challenges of Blockchain in the context of CPS and the IoT, identifying areas for potential improvement and innovation. Here are the key points:

- **Scalability**: The chapter discusses Blockchain's difficulty scaling up to accommodate increasing transactions and nodes.
- **Performance**: It addresses performance limitations affecting Blockchain network efficiency, particularly latency and throughput.
- **Security**: Despite Blockchain's secure design, the chapter acknowledges that it is not immune to security flaws and vulnerabilities.
- **Integration Complexity**: The complexities associated with integrating Blockchain with other systems, such as IoT devices, are highlighted as significant challenges5.

These limitations underscore the need for ongoing research and development to address practical implementation and scaling problems within Blockchain technology.

The third objective of the thesis was to develop a case-based BCoT architecture to facilitate the systematic collection of data from IoT devices through web services and data files, ensuring interoperability and efficient data management.

The thesis explores groundbreaking applications of Blockchain of Things (BCoT), machine learning, and educational technology across three key chapters. Chapter 4 delves into integrating IoT devices with Ethereum Blockchain, tackling the complex balance between Blockchain's security strengths and IoT hardware limitations. It outlines an innovative architecture utilising Raspberry Pi 4 devices as network nodes to connect IoT networks with Blockchain systems. The subsequent chapter evaluates this BCoT architecture's performance within a private Ethereum environment, examining crucial metrics like latency and throughput. Chapter 6 pivots to healthcare, presenting a novel machine-learning system for ICU patient monitoring. This system, built on a Random Forest classifier, shows impressive accuracy in condition prediction and early warning generation, potentially transforming intensive care data management and patient care approaches. Chapter 5 introduces the concept of "Lab Chain," a Blockchain-powered Learning Management System (LMS) for remote laboratory administration. This aligns with emerging Education 4.0 principles, harnessing Blockchain to provide secure, transparent, and decentralised educational resources and data management in remote lab settings. These chapters demonstrate a sophisticated fusion of Blockchain, IoT, and machine learning technologies. They address key scalability, latency, and security challenges across healthcare and education domains. The proposed systems showcase the transformative potential of these technologies in enhancing efficiency, security, and data management practices.

The fourth objective of this thesis was to implement a Blockchain-based storage model for BCoT-generated data, leveraging the IPFS for distributed storage while maintaining data chronology and integrity through Ethereum smart contracts.

Section 7.6 of the thesis investigates the implementation of IPFS as a storage model within Docker containers. This configuration leverages the IPFS Cluster's replication strategy and optimized network routing to enhance efficiency. The IPFS Cluster, when deployed in a Dockerized environment, offers several advantages including high availability, load balancing, redundancy, fault tolerance, and horizontal scalability. The section delineates the various roles within an IPFS Cluster, such as tracker and storage nodes, and explains the utilization of the Cluster REST API for management and monitoring purposes.

Performance analysis indicates that IPFS deployed in Docker containers demonstrates improved latency times and overall efficiency compared to standalone installations. The experimental design for evaluating IPFS performance involves testing read and write operations using file sizes ranging from 1 KB to 64 MB. This approach allows for a comprehensive assessment of how IPFS handles files of varying sizes, considering the system's method of splitting files into blocks, which particularly affects processing time for larger files. The study focuses on measuring latency during file operations in IPFS, providing valuable insights into the system's efficiency. Analysis of the results emphasizes the correlation between file size and IPFS performance and latency, offering crucial understanding of the practical implications within the context of the BCoT architecture.

The research compares the latency performance of IPFS in Docker environments for both writing and reading operations across different file sizes.

Findings indicate enhanced efficiency of IPFS when utilized within Docker containers, attributed to the IPFS Cluster's replication strategy and optimized network routing. The IPFS Cluster's role in providing high availability, load balancing, redundancy, fault tolerance, and scalability is highlighted. Experimental results demonstrate that IPFS performs more efficiently in Docker environments compared to standalone setups, exhibiting lower latency times for file operations. This research contributes to the understanding of IPFS performance in containerized environments and its potential applications in distributed storage systems.

The final objective of this thesis was to thoroughly validate the Blockchain-based proposed solution's scalability and performance characteristics. This is crucial to ensuring it meets the desired functional and performance requirements. This involves conducting comprehensive testing and analysis to assess the solution's ability to handle increasing workloads and maintain optimal performance under various conditions.

Chapter 7 of the thesis focuses on the performance analysis of the BCoT application. Following are the key takeaways:

- **BCoT Ecosystem:** The chapter discusses the setup and testing of a BCoT ecosystem on a trial platform, demonstrating its technical feasibility and appropriateness for specific IoT applications.
- **Stability and Metrics:** The BCoT, deployed on three RPi4 nodes, operated continuously, proving its stability and reliability. This performance instils confidence that even less powerful devices could meet the needs of the Blockchain network.
- **Resource Efficiency:** The chapter highlights the BCoT ecosystem's minimal disk space and resource needs, making it suitable for areas with limited network infrastructure.
- **Computational Resources:** Nodes have ample computational and memory resources, allowing them to handle additional tasks such as data acquisition without affecting Blockchain efficiency.

The chapter comprehensively analyses the BCoT application's performance, emphasising its potential for IoT applications and its adaptability to resource-constrained environments. It also includes specific example numbers related to latency measurements for IPFS operations, showcasing the system's responsiveness. Here are the key findings:

- **RPi4 Performance:** The chapter details experiments assessing the RPi4's average total time of transaction submission latency and average throughput in a private Ethereum network at different transaction volumes. For example, the study examined gas limit and gas price parameters, which affect transaction fees and overall throughput.
- **IPFS vs. FTP Latency**: The chapter compares the latency and resource utilisation of IPFS and FTP systems within Docker environments. The latency of IPFS was significantly greater than FTP, especially for large files, due to the additional tasks carried out during the IPFS writing process.
- **Docker-Cluster Containers:** The chapter highlights the potential and challenges of deploying IPFS in private networks within organisations. It suggests that IPFS performance in Docker-Cluster containers is promising, with a notable reduction in latency attributed to Docker's efficient resource utilisation.
- **Scalability and Efficiency:** The chapter concludes that the suggested BCoT system is technically feasible, scalable, and appropriate for real-world IoT applications due to its low-performance requirements and ability to use nodes for additional tasks without impacting Blockchain efficiency. The system's adaptability is emphasised, allowing IoT devices to function as Blockchain nodes and data collection endpoints.

These findings contribute to understanding the performance dynamics of Blockchain and IPFS technologies and their integration into IoT systems.

8.3 Limitations

Like any research, there are limitations in the proposed works and solutions, In this thesis, the limitations are as follows:

- **PoA is limited by the storage constraints of some IoT devices:** The utilization of PoA for direct Blockchain access by end devices is constrained by the storage limitations of certain IoT devices, particularly those in the sensing layer. These devices lack the capacity to store the complete Blockchain or even substantial portions of it, thereby restricting their ability to fully leverage the available data. This limitation poses challenges for implementing PoA in resource-constrained IoT environments and necessitates alternative approaches to enable effective data utilization across all network layers.

The implementation of PoA in IoT networks faces a significant challenge when it comes to end device access to the Blockchain. While PoA allows direct access to the entire Blockchain, this feature is severely limited by the storage constraints of many IoT devices, especially those in the sensing layer. These devices simply lack the capacity to store the complete Blockchain or even substantial portions of it. As a result, their ability to fully utilize the wealth of data available on the Blockchain is significantly restricted. This limitation highlights the need for alternative approaches or optimizations to enable effective data utilization across all layers of IoT networks employing PoA consensus mechanisms.

- **Real-world hurdles:** Implementing the novel architecture in a real hospital brings many challenges. Some of the obstacles that need to be considered are the sheer complexity of integrating it with existing hospital infrastructure, abiding by regulatory standards of healthcare information systems, and making it interoperable with other medical systems.
- **Scalability of PoA:** Although our modifications improve the scalability, it is still a big challenge to process massive transactions (eg, thousands per second) and to achieve high throughput in huge distributed applications with millions of IoT devices. The improved PoA mechanism still might not be efficient enough in extreme cases. These shortcomings do not invalidate the improvements put forth in this thesis but likely point to directions for future research and optimisations. Further research should look to improve the scalability of the PoA mechanism, perhaps through hybrid schemes or more lightweight layer-2 solutions, to tackle these issues for large-scale IoT deployments.
- **Edge Computing Resource Constraints:** The computational and energy resources within edge devices might limit the integration of AI and Blockchain on devices,

making them unable to perform complex AI model inference and Blockchain operations.

- **Interoperability Challenges:** Moreover, the convergence of multiple technologies (IoT, Blockchain, AI, IPFS) might pose interoperability challenges, especially when interfacing with legacy systems in healthcare (or other industries at large).
- **Security and Privacy Concerns:** Although Blockchain increases security, the entire system is as strong as its weakest link. If a backdoor is found in an IoT device or another edge node, that can compromise the whole architecture.

8.4 Future Work

Future research is essential to enhance and expand BCoT architectures, particularly in their applications within education and various industries. A promising strategy to improve scalability involves simulating real-world conditions by increasing the number of nodes and transactions in test environments. This approach enables researchers to evaluate performance under heavier workloads, identify bottlenecks within the architecture, and propose optimisations to boost system efficiency. Suggested methods include adaptive node clustering and dynamic load balancing mechanisms to manage high transaction volumes effectively.

Additionally, integrating decentralised predictive analytics and decision-making through advanced AI and machine learning techniques represents a significant area for future development. By incorporating AI-driven algorithms, BCoT systems can analyse large datasets in real time, enhancing responsiveness and accuracy in applications such as healthcare and education. Researchers should focus on developing decentralised machine learning frameworks that support real-time model updates and distributed analytics across the Blockchain network, further elevating system intelligence and adaptability.

Strengthening the security of IoT devices connected to BCoT systems is paramount. Future research should prioritise developing advanced security protocols tailored to combat specific vulnerabilities in IoT environments. Solutions like lightweight cryptographic methods, Blockchain-based intrusion detection systems, and zero-trust security frameworks could enhance protection without compromising performance.

Moreover, promoting interoperability among individual Blockchain platforms and IoT devices is crucial for fostering a more integrated BCoT ecosystem. Investigating cross-chain communication protocols and interoperability standards would facilitate seamless interactions between diverse Blockchain networks and IoT devices, creating a cohesive and flexible BCoT ecosystem applicable across multiple domains. Researchers could explore Blockchain-agnostic solutions that allow different Blockchains to share information and resources while preserving their unique architectures.

Overall, this research lays the groundwork for future studies in smart cities, supply chain management, and environmental monitoring, showcasing how BCoT can improve efficiency, transparency, and sustainability. Building on these findings, subsequent research can significantly advance BCoT technology, creating more robust and efficient systems across diverse fields.

References

Abadi, F. A., Ellul, J. & Azzopardi., G., 2018. The Blockchain of Things, Beyond Bitcoin: A Systematic Review. 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),, pp. 1666-1672, doi: 10.1109/Cybermatics_2018.2018.00278..

Abbas, A., Hosseini, S., Núñez, J. & Sastre-Merino, S., 2021. Emerging technologies in education for innovative pedagogies and competency development. Australasian Journal of Educational Technology, pp. 1-1, https://doi.org/10.14742/ajet.7680.

Abdullah Lajam, O. a. T. A. H., 2021. Performance Evaluation of IPFS in Private Networks. 4th International Conference on Data Storage and Data Engineering.

Adeghe, E. P., Okolo, C. A. & Ojeyinka., O. T., 2024. Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes.,. Open Access Research Journal of Science and Technology, 2024, 10(02), 013–020., pp. 1, https://doi.org/10.53022/oarjst.2024.10.2.0044.

Ahakonye, L., Nwakanma, C. & Kim, D., 2024. Tides of Blockchain in IoT Cybersecurity.. Sensors, [online], (24)((10)), pp. 3111, https://doi.org/10.3390/s24103111..

Ahmad, A. P., Ilham, A. A. & Paundu., A. W., 2023. Analysis of Blockchain and Interplanetary File System (IPFS) Utilization for Big Data Architecture Optimization,. IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), pp. 652-657, Doi: 10.1109/COMNETSAT59769.2023.10420785..

Ahmed G. Gad, D. T. M. L. A. A. A. A., 2022. Emerging Trends in Blockchain Technology and Applications: A Review and Outlook. Journal of King Saud University - Computer and Information Sciences, Issue ISSN 1319-1578.

Aich, S. et al., 2019. A Review on Benefits of IoT Integrated Blockchain Based Supply Chain Management Implementations across Different Sectors with Case Study. 21st International Conference on Advanced Communication Technology (ICACT), pp. 138–141, https://doi.org/10.23919/ICACT.2019.8701910.

Alammary, A., Alhazmi, S., Almasri, M. & Gillani., S., 2019. Blockchain-Based Applications in Education: A Systematic Review. Applied Sciences, Volume (7), pp. 2-18, https://doi.org/10.3390/app9122400.

Alam, S. et al., 2023. An Overview of Blockchain and IoT Integration for Secure and Reliable Health Records Monitoring. Sustainability 15, Issue (7), pp. 1-1, https://doi.org/10.3390/su15075660..

Alam, T., 2020. Blockchain-based big data analytics approach for smart cities. Technology Reports of Kansai University, (62)((9)), pp. 45-61, https://doi.org/10.36227/techrxiv.13054244.v1.

Alam, T., 2020. Performance Evaluation of Blockchains in the Internet of Things. Computer Science and Information Technologies., Issue (2722-3221), pp. 93-97, DOI: 10.11591/csit.v1i2.

Alam, T., 2023. Blockchain-Based Internet of Things: Review, Current Trends, Applications, and Future Challenges. Computers 12, Issue (1: 6), pp. 1-1, https://doi.org/10.3390/computers12010006.

Aleskerov, E., B, F. & B., R., 1997. Cardwatch: A neural network-based database-mining system for credit card fraud detection.. Computational Intelligence for Financial Engineering (CIFEr),Proceedings of the IEEE/IAFE 1997, p. 220–6..

Al-hajjar, A. & Al-Qurabat, A., 2023. An overview of machine learning methods in enabling IoMT-based epileptic seizure detection.. The Journal of Supercomputing, 79(14), 16017-16064, (79)((14)), pp. 16017-16064, https://doi.org/10.1007/s11227-023-05299-9.

Alhamzah, A. et al., 2022. The Blockchain Technologies in Healthcare: Prospects, Obstacles, and Future Recommendations; Lessons Learned from Digitalization.. International Journal of Online and Biomedical Engineering (iJOE), (18)((09)), pp. 144–159, https://doi.org/10.3991/ijoe.v18i09.32253.

Ali, A. et al., 2023. Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning.. Sensors, pp. 1, https://doi.org/10.3390/s23187740.

Ali, A. et al., 2022. An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network.. Sensors, pp. 1-1, https://doi.org/10.3390/s22020572.

Alkadi, O., Moustafa, N., Turnbull, B. & Choo, K.-K. R., 2021. A Deep Blockchain Framework-Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks. IEEE Internet of Things Journal, (8)((12)), pp. 1-1, https://doi.org/10.3390/app9122400.

Alkhaldi, T., Pranata, I. & Athauda., R. I., 2016. A Review of Contemporary Virtual and Remote Laboratory Implementations: Observations and Findings. Journal of Comput-ers in Education, Volume (3), pp. 329–351, https://doi.org/10.1007/s40692-016-0068-z.

Alkhammash, M., 2022. A Blockchain and IoT based&nbsp; Framework for Decentralised Smart Campus Environments. Ph.D Thesis, pp. 1-181.

Alkhateeb, A., Catal, C., Kar, G. & Mishra., A., 2022. Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review.. Sensors (Basel)., pp. 1-1, doi: 10.3390/s22041304. PMID: 35214212; PMCID: PMC8962977..

Allam, A. H., Gomaa, I., Zayed, H. H. & Taha., M., 2024. IoT-based eHealth using blockchain technology: a survey.,. Cluster Comput, pp. 1-1, https://doi.org/10.1007/s10586-024-04357-y.

Ally, M. & Wark, N., 2019. Learning for Sustainable Development in the Fourth Industrial Revolution. Commonwealth of Learning, Volume (9).

Almalki, J., 2024. State-of-the-Art Research in Blockchain of Things for HealthCare.. Arab J Sci Eng 49, pp. 3163–3191, https://doi.org/10.1007/s13369-023-07896-5.

Al-Nbhany, W., Zahary, A. T. & Al-Shargabi., A. A., 2024. Blockchain-IoT Healthcare Applications and Trends: A Review,. IEEE Access, Volume (12), pp. 4178-4212, doi: 10.1109/ACCESS.2023.3349187.

Alrubei, S. J. R. C. W. a. E. B., 2019. Ethereum Blockchain for Securing the Internet of Things: Practical Implementation and Performance Evaluation. International Conference on Cyber Security and Protection of Digital Services (Cyber Security), p. pp. 1–5.

Alrubei, S. M., Ball, E. & Rigelsford., J. M., 2022. A Secure Blockchain Platform for Supporting AI-Enabled IoT Applications at the Edge Layer. IEEE Access, Volume (10), pp. 18583-18595, doi: 10.1109/ACCESS.2022.3151370.

AlSadawi, A., Hassan, M. S. & Ndiaye., M., 2021. A Survey on the Integration of Blockchain with IoT to Enhance Performance and Eliminate Challenges. IEEE Access, Volume (9), pp. 54478–54497, https://doi.org/10.1109/ACCESS.2021.3070555.

Al-Zoubi, A., Aldmour, M. & Aldmour., R., 2022. Blockchain as a learning management system for laboratories 4.0. International Journal of Online and Biomedical Engineering, (18)((12)), pp. 1-1, Doi: 10.3991/ijoe.v18i12.33515..

Amiri, Z. et al., 2024. The applications of nature-inspired algorithms in Internet of Things-based healthcare service: A systematic literature review.. Transactions on emerging telecommunications technologies,, (35)((6)), pp. 1, https://doi.org/10.1002/ett.4969.

Anderlini, D. et al., 2023. From Gilgamesh's quest for immortality to everlasting cloud hyper-collective mind: ethical implications for artificial intelligence. Global Knowledge, Memory and Communication, (72)((6/7)), pp. 648-665, https://doi.org/10.1108/GKMC-08-2021-0130.

Anil, K. .. & Kamble, M., 2023. Health Block: A Blockchain Based Secure Healthcare Data Storage and Retrieval System for Cloud Computing.. International Journal on Recent and Innovation Trends in Computing and Communication,, (11)((9)), pp. 96–104, https://doi.org/10.17762/ijritcc.v11i9.8324.

Anon., 2018. University, Woolf: The First Blockchain. pp. 1-1, https://www.docdroid.net/ebIGXJm/whitepaper3-pdf.

Ansari, M. N. et al., 2013. Primary Non-Hodgkin's Lymphoma of Stomach: To report 54 patients and Analysis of Major Reported Series..

Anyanwu, A., 2024. Integrating IoT with virtual healthcare: a theoretical framework for enhancing accessibility and efficiency in the U.S. healthcare sector.. GSC Advanced Research and Reviews,, (18)((3)), pp. 043-049, https://doi.org/10.30574/gscarr.2024.18.3.0087.

Arachchige, K. G., Branch, P. & Jason., B., 2023. Evaluation of Blockchain Networks' Scalability Limitations in Low-Powered Internet of Things (IoT). Sensor Networks. Future Internet, pp. 15- 31, https://doi.org/10.3390/fi15090317.

Arul, P. & Renuka., S., 2023. Preserving the Privacy of the Healthcare, Clinical and Personal Data using Blockchain.. Indian Journal of Science and Technology., (16)((1)), pp. 23-31, https://doi.org/10.17485/IJST/v16i1.1842.

Asad, M. M. et al., 2022. Investigating the impact of IoT-Based smart laboratories on students' academic performance in higher education.. Univers Access Inf Soc., pp. 1-15, doi: 10.1007/s10209-022-00944-1..

Asad, N., Elahi, M., Hasan, A. & Yousuf, M., 2020. Permission-Based Blockchain with Proof of Authority for Secured Healthcare Data Sharing.. 2nd International Conference on Advanced Information and Communication Technology (ICAICT), pp. 35-40, https://doi.org/10.1109/ICAICT51780.2020.9333488.

Atadoga, A. et al., 2024. Blockchain in healthcare: A comprehensive review of applications and security concerns. International Journal of Science and Research Archive, 11(01), 1605–1613., pp. 1, https://doi.org/10.30574/ijsra.2024.11.1.0244.

Atienza-Mendez, C. & Bayyou., D. G., 2019. Blockchain Technology Applications in Education. International Journal of Computing and Technology, (6)((11)).

Atlam, H., Alenezi, A., Alassafi, M. O. & Wills., G. B., 2018. Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. International Journal of Intelligent Systems and Applications, Volume (6), pp. 40–48, https://doi.org/10.5815/ ijisa.2018.06.05.

Attaran, M., 2020. Blockchain technology in healthcare: Challenges and opportunities,. International Journal of Healthcare Management, (15)(1), pp. 70-83, DOI: 10.1080/20479700.2020.1843887.

Auer, M. E., Azad, A. K., Edwards, A. & Jong., T. d., 2019. Cyber-Physical Laboratories in Engineering and Science Education. Springer International Publishing, Issue ISBN: 978-3-319-76934-9, Electronic ISBN: 978-3-319-76935-6., pp. 1-1, https://doi.org/ 10.1007/978-3-319-76935-6.

Badidi, E., 2022. Edge AI and Blockchain for Smart Sustainable Cities: Promise and Potential. Sustainability 14, Issue (13), pp. 1-1, https://doi.org/10.3390/su14137609.

Baig, M. A. et al., 2022. A Study on the Adoption of Blockchain for IoT Devices in Supply Chain. Comput Intell Neurosci., pp. 1-1, Doi: 10.1155/2022/9228982. PMID: 35909824; PMCID: PMC9325587..

Bajcsy, R., Lee, S. & Leonardis, A., 1990. Colour image segmentation with detection of highlights and local illumination induced by inter-reflections. In: Proceedings of ICPR, pp. 785-790.

Barnard, K., Cardei, V. & Funt, B., 2002. A comparison of computational color constancy algorithms. I: Methodology and experiments with synthesized data. In: IEEE Transactions on Image Processing, 11(9), pp. 972-984.

Bashar Hammad., A. A.-Z. M. C., 2020. Harnessing Technology in Collaborative Renewable Energy Education. International Journal of Ambient Energy, Vol. 41(No. 10), p. pp. 1118–1125.

Bastien Confais, A. L. a. B. P., 2017. Performance Analysis of Object Store Systems in a Fog and Edge Computing Infrastructure. Transactions on Large-Scale Data-and Knowledge-Centered Systems XXXIII. Springer, pp. 40-79.

Berns, R. S., Motta, R. J. & Gorzynski, M. E., 1993. CRT colorimetry. Part I: Theory and practice. Color Re- search & Application, 18(5), pp. 299-314.

Bhadula, S., Sharma, S. & Johri., A., 2023. Hybrid Blockchain and IPFS for Secure Industry 4.0 Framework of IoT-based Skin Monitoring System. 9th International Conference on Advanced Computing and Communication Systems (ICACCS),, pp. 41-47, Doi: 10.1109/ICACCS57279.2023.10112751.

Bhawana & Kumar., S., 2021. A Review on Cyber-Physical Systems based on Blockchain: Possibilities and Challenges. IEEE 6th International Conference on Computing, Communication and Automation (ICCCA), pp. 691-696 ,https://doi.org/10.1109/ICCCA52192.2021.9666299.

Burgos, J. B. & Pustišek, M., 2024. Decentralized IoT Data Authentication with Signature Aggregation.. Sensors, (24)((3)), pp. 1037–1037, https://doi.org/10.3390/s24031037.

Burt, P. J. & Adelson, E. H., 1983. The Laplacian Pyramid as a Compact Image Code. In: IEEE Transaction on Communications, 31(4), pp. 532-540.

Calik, E. & Bendechache, M., 2024. Blockchain for Organ Transplantation: A Survey.,. Blockchains, pp. 150-172, https://doi.org/10.3390/blockchains2020008.

Cao, G., Zhao, Y., Ni, R. & Li, X., 2014. Contrast enhancement-based forensics in digital images. IEEE transactions on information forensics and security, 9(3), pp. 515-525.

Cardei, V., Funt, B. & Barnard, K., 2002. Estimating the scene illumination chromaticity using a neural network. In: Journal of the Optical Society of America A, 19(12), pp. 2363-2373.

Carreras, F., Delgado, Á., García-Serrano, J. & Medina-Quero, J., 2017. A virtual model of the retina based on histological data as a tool for evaluation of the visual fields.

Casino, F., Dasaklis, T. K. & Patsakis., C., 2019. A systematic literature review of blockchain-based applications: Current status, classification and open issues,. Telematics and Informatics,, (36)((0736-5853)), pp. 55-81, https://doi.org/10.1016/j.tele.2018.11.006..

Castro, R. & Yong-Oliveira, M. A., 2021. Blockchain and Higher Education Diplomas. European Journal of Investigation in Health, Psychology and Education, Volume (11), pp. 154–167, https://doi.org/10.3390/ejihpe11010013.

Chacon, J. et al., 2015. EJS, JIL Server, and LabVIEW: An Architecture for Rapid Development of Remote Labs. IEEE Transactions on Learning Technologies, (8)((4)), pp. 393–401, https://doi.org/10.1109/TLT.2015.2389245.

Chand, M. et al., 2024. Multi-layer Security and Power Efficiency Improvement with Blockchain Technology and NB-IoT.. Research Square (Research Square), pp. 1, https://doi.org/10.21203/rs.3.rs-4111246/v1.

Chang, K.-m. K. & Rocke., A. J., 2021. A Global History of Research Education:Disciplines,Institutions,and Nations,1840–1950:. (18)((12)).

Chan, K. C. et al., 2019. Integration of Blockchains with Management Information Systems. International Conference on Mechatronics, Robotics and Systems Engineering (MoRSE), pp. 157–162, https://doi.org/10.1109/MoRSE48060.2019.8998694.

Cha, S. C. C. J. F. S. C. &. Y. K. H., 2018. A Blockchain Connected Gateway for BLEBased Devices in the Internet of Things.. IEEE Access, Volume vol. 6, p. pp. 24639–24649.

Cheng, J.-C., Lee, N.-Y., Chi, C. & Chen, Y.-H., 2018. Blockchain and Smart Contract for Digital Certificate. Proceedings of IEEE International Conference on Applied System Innovation, Taiwan, pp. 1-1, https://doi.org/10.1109/ICASI.2018.8394455.

Chen, X., K., N. & Sekiya, H., 2021. An experimental study on performance of private blockchain in IoT applications.. Peer-to-Peer Networking and Applications., pp. 3075-3091, https://doi.org/10.1007/s12083-021-01148-9.

Chen, X., Nakada, R., Nguyen, K. & Sekiya., H., 2021. A Comparison of Distributed Ledger Technologies in IoT: IOTA versus Ethereum. 20th International Symposium on Communications and Information Technologies (ISCIT), pp. 182–187, https://doi.org/10.1109/ISCIT52804.2021.9590601.

Chen, X. N. K. a. S. H., 2021. An experimental study on the performance of private blockchain in IoT Applications,. Peer-to-Peer Networking and Applications,, p. pp. 3075–3091..

Chen, Y. et al., 2019. Blockchain-based medical records secure storage and medical service framework. Journal of Medical Systems, pp. 1-1, https://doi.org/10.1007/s10916-018-1121-4.

Chowdhury, M. J. M. et al., 2019. A Comparative Analysis of Distributed Ledger Technology Platforms. IEEE Access. 7., pp. 167930-167943, DOI:10.1109/ACCESS.2019.2953729.

Ciurea, F. & Funt, B., 2004. Tuning retinex parameters. In: Journal of Electronic Imaging, 13(1), pp. 58-64.

Clifton, L. et al., 2013. Gaussian processes for personalized e-health monitoring with wearable sensors.. IEEE Trans Biomed Eng., pp. 60 (1):193-7, doi: 10.1109/TBME.2012.2208459.

Confais, B., Lebre, A. & Parrein., B., 2017. An object store for Fog infrastructures based on IPFS and a Scale-Out NAS. RESCOM 2017, Issue 2, pp. 1, https://doi.org/10.1109/ICFEC.2017.13.

Conoscenti, M., Vetrò, A. & Martin., J. C. D., 2016. Blockchain for the Internet of Things: A Systematic Literature review. IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–6, https://doi.org/10.1109/ AICCSA.2016.7945805.

Correia, R. C., Alves, G. R. & Fonseca., J. M., 2021. An Evolution Model for Remote and Virtual Labs. 4th International Conference of the Portuguese Society for Engineering Edu-cation (CISPEE), pp. 1–10, https://doi.org/10.1109/CISPEE47794.2021.9507222.

Coskun, S., Kayıkcı, Y. & Gençay., E., 2019. Adapting Engineering Education to Industry 4.0 Vision. Technologies, (7)((10)), pp. 1–13, https://doi.org/10.3390/technologies7010010.

Coskun, S., Kayıkcı, Y. & Gençay, E., 2019. Adapting Engineering Education to Industry 4.0 Vision. Technologies, (7)((10)), pp. 1-13, https://doi.org/10.3390/technologies7010010.

Cui, H. et al., 2019. IoT Data Management and Lineage Traceability: A Blockchain-based Solution,. IEEE/CIC International Conference on Communications Workshops in China (ICCC Workshops),, pp. 239-244, doi: 10.1109/ICCChinaW.2019.8849969..

Dai, H., Zheng, Z. & Zhang., Y., 2019. Blockchain for Internet of Things: A Survey. IEEE Internet of Things Journal, (6)((5)), pp. 8076–8094, https://doi.org/10.1109/ JIOT.2019.2920987.

Danilo, G. Z., E, A. M. & Al-Zoubi, A., 2009. Design and Verification of Application-Specific Integrated Circuits in a Network of Remote Labs. International Journal of Online Engineering (iJOE), (5)((3)), pp. 25–29, https://doi.org/10.3991/ijoe.v5i3.690.

Darwish, D. G., 2018. Improved Layered Architecture for Internet of Things. International Journal of Computing Academic Research (IJCAR), (6)((2)), pp. 214–223, http://meacse.org/IJCAR/archives/71.pdf.

Devi, M. S., Suguna, R. & Abhinaya, P., 2019. Integration of Blockchain and IoT in Satellite Monitoring Process.,. IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1-6, https://doi.org/10.1109/ICECCT.2019.8869185.

Do Hai Son, T. T. T. Q. T. V. K. D. T. H. N. L. T. N. V. H. D. N. D. N. N. a. E. D., 2021. An Effective Frame-work of Private Ethereum Blockchain Networks for Smart Grid. International Conference on Advanced Technologies for Communications (ATC), p. pp. 312–317.

Domínguez-Bolaño, T. et al., 2022. An overview of IoT architectures, technologies, and existing open-source projects. Internet of Things,, (20)((2542-6605)), pp. 1-1, https://doi.org/10.1016/j.iot.2022.100626.

Dorri, A., Kanhere, S. S. & Jurdak., R., 2016. Blockchain in Internet of Things: Challenges and Solutions. pp. 1-1, https://doi.org/10.48550/arXiv.1608.05187.

Dorri, A., Kanhere, S. S., Jurdak, R. & Gauravaram., P., 2017. Blockchain for IoT security and privacy: The case study of a smart home,. IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618-623, Doi: 10.1109/PERCOMW.2017.7917634..

D, S. & Maragatham., G., 2021. Movie Rating System based on Blockchain. International Conference on Computer Communication and Informatics (ICCCI), pp. 1–3, https://doi.org/10.1109/ICCCI50826.2021.9402381.

Eisenbarth, J.-P., Cholez, T. & Perrin., O., 2022. Ethereum's Peer-to-Peer Network Monitoring and Sybil Attack Prevention. Journal of Network and Systems Management, Special Issue on Blockchains and Distributed Ledgers in Network and Service Management, pp. 65, Doi:10.1007/s10922-022-09676-2.

El-dosuky, M. A. & Eladl., G. H., 2019. E-Learning Framework Based on Blockchain Technology. International Journal of Computer Science and Network, (8)((6)), pp. pp. 466–473,.

Fernando, E., Meyliana & Surjandy, 2019. Blockchain Technology Implementation in Raspberry Pi for Private Network. International Conference on Sustainable Informa- tion Engineering and Technology (SIET), pp. 154–158 , https://doi.org/10.1109/ SIET48054.2019.8986053.

Finlayson, G. D., 1995. Color constancy in diagonal chromaticity space. In: Proceedings of the Fifth International IEEE Conference on Computer Vision, pp. 218-223.

Frerich, S. et al., 2016. Engineering Education 4.0: Excellent Teaching and Learning in Engineering Sciences. Springer International Publishing, Issue ISBN: 978-3-319-469157, Electronic ISBN: 978-3-319-46916-4., pp. 1-1, https://link.springer.com/book/10.1007%2F978-3-319-46916-4.

Fu, X. et al., 2016. A fusion-based enhancing method for weakly illuminated images. Signal Processing, Volume 129, pp. 82-96.

Gabriel, D., 2013. Inductive and deductive approaches to research, Accessed on “28/02/2024. Inductive and deductive approaches to research .

Garcia-Loro, F. et al., 2021. Laboratories 4.0: Laboratories for Emerging Demands under Industry 4.0 Paradigm. 2021 IEEE Global Engineering Education Confer-ence (EDUCON), pp. 903–909, https://doi.org/10.1109/EDUCON46332.2021.9454095.

Georgeson, M. A. & Sullivan, G. D., 1975. Contrast constancy: deblurring in human vision by spatial frequency channels. In: The Journal of Physiology, 252(3), pp. 627-656.

Gerald, I., Manuel, M. & Salvatore., D., 2022. Smart Parking Solution for Enterprise on Ethereum.. pp. 1-6, Doi:10.1109/NIR52917.2021.9666126.

Gonschor, D., Jung, M., Costa, J. & Brandl, R., 2022. Remote Hardware-in-the-Loop Laboratory and its Application in Engineering Education. IEEE Global Engineering Education Conference (EDUCON), pp. 1959-1964, https://doi.org/10.1109/EDUCON52537.2022.9766816.

Guerra, J. et al., 2022. Design and Evaluation of a Heterogeneous Lightweight Blockchain-Based Marketplace. Sensors (Basel)., pp. 1-1, doi: 10.3390/s22031131. PMID: 35161877; PMCID: PMC8840334..

Guinaldo, M., Torre, L. d. l., Heradio, R. & Dormido., S., 2013. Virtual and Remote Control Laboratory in Moodle: The Ball and Beam System. 10th IFAC Sympo-sium Advances in Control Education, The International Federation of Automatic Control.

Gulia, D. P. et al., 2024. Exploring the Potential of Blockchain Technology in an IoT-Enabled Environment: A Review.. IEEE Access, pp. 1-1..

Guo, X., Li, Y. & Ling, H., 2016. LIME: Low-light image enhancement via illumination map estimation. IEEE Transactions on Image Processing, 26(2), pp. 982-993.

Habib, G. et al., 2022. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing.. Future Internet, pp. 1-1, https://doi.org/10.3390/fi14110341.

Halili., S. H., 2019. Technological Advancements in Education 4.0. The Online Journal of Distance Education and e-Learning, (7)((1)), pp. 1-1, http://tojdel.net/journals/tojdel/articles/v07i01/v07i01-08.pdf.

Hammad, B., Al-Zoubi, A. & Castro., M., 2020. Harnessing Technology in Collaborative Renewable Energy Education. International Journal of Ambient Energy, (41)((10)), pp. 1118–1125, https://doi.org/10.1080/01430750.2018.1501751.

Handayani, I. et al., 2023. Enhancing Security and Privacy of Patient Data in Healthcare: A SmartPLS Analysis of Blockchain Technology Implementation.. IAIC Transactions on Sustainable Digital Innovation (ITSDI), (5)((1)), pp. 8–17, https://doi.org/10.34306/itsdi.v5i1.603.

Hang, L. & Kim., D.-H., 2019. Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. Sensors 19, Issue (10: 2228), pp. 1-1, https://doi.org/10.3390/s19102228.

Hao, Y. Y. L. X. D. L. F. a. P. C., 2018. Performance Analysis of Consensus Algorithm in Private Blockchain. IEEE Intelligent Vehicles Symposium (IV), p. pp. 280–285.

Haque, E. et al., 2024. A scalable blockchain based framework for efficient IoT data management using lightweight consensus.. Scientific Reports., pp. 1-1, doi: 10.1038/s41598-024-58578-7.

Hautière, N., Tarel, J., Aubert, D. & Dumont, E., 2008. Blind contrast enhancement assessment by gradient ratioing at visible edges. Image Analysis & Stereology, 27(2), pp. 87-95.

Hegde, P. & Maddikunta, P., 2023. Amalgamation of blockchain with resource-constrained IOT devices for healthcare applications – state of the art, challenges and Future Directions. International Journal of Cognitive Computing in Engineering,, pp. 220–239, doi:10.1016/j.ijcce.2023.06.002..

Hieu, D. a. K. L., 2021. A Fast Keccak Hardware Design for High Performance Hashing System. 15th International Conference on Advanced Computing and Applications (ACOMP), p. pp. 162–168.

Hirschi., A., 2018. The Fourth Industrial Revolution: Issues and Implications for Career Research and Practice. Career Development Quarterly, Volume (66), pp. 192–204, https://doi.org/10.1002/cdq.12142.

Ho, J., Funt, V. & Drew, M. S., 1990. Separating a color signal into illumination and surface reflectance components: Theory and applications. In: IEEE Transactions on Pattern Analysis and Machine Intelligence, 12(10), pp. 966-977.

Hou, Y., Liu, Y., Luo, M. & Xu., W., 2020. An architecture for smart university data collection and management based on blockchain network. Chinese Automation Congress (CAC), pp. 4317-4322, doi: 10.1109/CAC51589.2020.9326577..

Huang, H.-S., T.-S, C. & J.-Y., W., 2020. A secure file sharing system based on IPFS and Blockchain,. Proceedings of the 2020 2nd International Electronics Communication Conference, pp. 1-1, Doi:10.1145/3409934.3409948..

Huang, X., Xu, C., Wang, P. & Liu, H., 2018. a security model for electric vehicle and charging pile management based on blockchain ecosystem.. IEEE Access, pp. 13565-13574, https://doi.org/10.1109/access.2018.2812176.

Hu, L., 2022. Intelligent value added service platform of smart library based on blockchain technology. IEEE International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA), pp. 1391-1394, doi: 10.1109/EEBDA53927.2022.9744776..

Hunt, R., 1982. A model of colour vision for predicting colour appearance. Color research & application, 7(2), pp. 95-112..

Hunt, R., 2004. The Reproduction of Color. 6th ed. England: Kingstonupon-Thames, Fountain Press.

Hussein, Z., Salama, M. & El-Rahman, S., 2023. Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms.. Cybersecurity, pp. 1, https://doi.org/10.1186/s42400-023-00163-y.

Hussin., A. A., 2018. Education 4.0 Made Simple: Ideas for Teaching. International Journal of Education and Literacy Studies,, (6)((3)), pp. 92–98, https://doi.org/10.7575/aiac.ijels.v.6n.3p.92.

Islam, M., Merlec, M. & In, H., 2022. A Comparative Analysis of Proof-of-Authority Consensus Algorithms: Aura vs Clique.. IEEE International Conference on Services Computing (SCC),, pp. 327-332, https://doi.org/10.1109/SCC55611.2022.00054.

Jaleel, A., Islam, S., Shahzad, M. & Affum, E., 2023. IoMT meets machine learning: from edge to cloud chronic diseases diagnosis system.. Journal of Healthcare Engineering, pp. 1-13, https://doi.org/10.1155/2023/9995292.

Jandrić, P., 2020. Postdigital Knowledge Socialism. In: Peters, M.A., Besley, T., Jandrić, P., Zhu, X. (eds) Knowledge Socialism.. East-West Dialogues in Educational Philosophy and Theory. Springer, pp. 1-1, https://doi.org/10.1007/978-981-13-8126-3_5.

Jan, Z. et al., 2018. A review on automated diagnosis of malaria parasite in microscopic blood smears images.. Multimedia Tools and Applications, 77(8), pp. 9801-9826.

Jean-Philippe, E., Cholez, T. & Perrin., O., 2023. Avoiding the 1 TB Storage Wall: Leveraging Ethereum's DHT to Reduce Peer Storage Needs. The 5th ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI 2023), ACM ASIACCS Workshop, pp. 10, Doi:10.1145/3594556.3594625..

Jentzsch, C., 2016. Decentralized Autonomous Organization to Automate Governance. White Paper, pp. 1–30, https://lawofthelevel.lexblogplatformthree.com/wp-content/uploads/sites/187/2017/07/WhitePaper-1.pdf.

Junfithrana, A. et al., 2018. Rice Donation System in Orphanage Based on Internet of Things, Raspberry-Pi, and Blockchain. International Conference on Computing, Engineering, and Design (ICCED), pp. 235–238, https://doi.org/10.1109/ICCED.2018.00053.

Kamal, N., Saad, M. M., Kok, C. & Hussain., A., 2018. Towards revolutionizing STEM education via IoT and blockchain technology. International Journal of Engineering and Technology, Volume (7), pp. 189-192, https://doi.org/10.14419/ijet.v7i4.11.20800..

Kamangar, Z. U., Memon, R. A., Memon, G. M. & Kamangar., U. A., 2023. Integration of Internet of Things and blockchain technology in healthcare domain: A systematic literature review.. Int J Commun Syst, pp. 1, doi:10.1002/dac.5582.

Kaur, S., Chaturvedi, S., Sharma, A. & Kar, J., 2021. A Research Survey on Applications of Consensus Protocols in Blockchain.. Secur. Commun. Networks,, pp. 1-1, https://doi.org/10.1155/2021/6693731..

Kee, E., Ting, H. Y. & Atanda., A. F., 2024. Enhancing Supply Chain Traceability through Blockchain and IoT Integration: A Comprehensive Review.. Green Intelligent Systems and Applications, (4)((1)), pp. 11–28, https://doi.org/10.53623/gisa.v4i1.355..

Ken Goldberg, M. M. S. G. N. R. C. S. a. J. W., 1995. Desktop Teleoperation via the World Wide Web. Proceedings of 1995 IEEE International Conference on Robotics and Automation, Volume Vol. 1, p. pp. 654–659.

Khalil, A. et al., 2021. A Literature Review on Blockchain-enabled Security and Operation of Cyber-Physical Systems.. 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1774-1779.

Khandelwal, P., Johari, R., Gaur, V. & Vashisth., D., 2021. BlockChain Technology based Smart Contract Agreement on REMIX IDE. 8th International Conference on Signal Processing and Integrated Networks (SPIN), pp. 938-942, doi: 10.1109/SPIN52536.2021.9565983..

Kim, E., Kim, W. & Lee, Y., 2003. Combination of multiple classifiers for the customer's purchase behavior prediction.. Decision Support Systems, pp. 167-175, https://doi.org/10.1016/S0167-9236 (02)00079-9.

Kim, T., 2024. A study on impact of lightweight cryptographic systems on internet of things-based applications.. Asia-Pacific Journal of Convergent Research Interchange,, (10)((1)), pp. 49-59, https://doi.org/10.47116/apjcri.2024.01.05.

Kim, W., Kwak, A., Yoo, B. & Ko., H., 2024. IPFS Viewer: IoT Surveillance Camera System Using IPFS and MQTT,. IEEE International Conference on Consumer Electronics (ICCE), pp. 1-6, Doi: 10.1109/ICCE59016.2024.10444244..

Kishor, R., 2023. Smart contract based fraud degree detection system.. Interantional Journal of Scientific Research in Engineering and Management,, (07)((08)), pp. 1, https://doi.org/10.55041/ijsrem25030.

Klinker, G. J., Shafer, S. A. & Kanade, T., 1990. A physical approach to color image understanding. In: International Journal of Computer Vision, 4(1), pp. 7-38.

Košťál, K. et al., 2019. Management and Monitoring IoT Devices Using Blockchain. Sensors 19, Issue (4), pp. 1-1, https://doi.org/10.3390/s19040856..

Krajčo, K., Habánik, J. & Grenčíková., A., 2019. The Impact of New Technology on Sustainable Development. Engineering Economics, (30)((1)), pp. pp. 41–49,.

Kumar., B., Albusaidi, I. & Halloush, M., 2023. Healthcare information exchange using blockchain and machine learning. Proceedings of the 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022), pp. 55–69, doi:10.2991/978-94-6463-110-4_6..

Kumar, M., 2024. Opportunities and challenges in the implementation of IoT applications for health monitoring of elderly people in the indian scenario.. Int Res J Adv Engg Hub, (2)((03)), pp. 425-430, https://doi.org/10.47392/irjaeh.2024.0062.

Kumar, P., Gupta, M. & Kumar., R., 2023. mproved Cloud Storage System Using IPFS for Decentralised Data Storage,. International Conference on Data Science and Network Security (ICDSNS), pp. 01-06, Doi: 10.1109/ICDSNS58469.2023.10245317.

Kumarswamy, S. & Athikatte., S. P., 2024. A Review of Blockchain Applications and Healthcare Informatics. International Journal of Safety and Security Engineering, pp. 267-287, https://doi.org/10.18280/ijsse.140127.

Kushwaha, S. et al., 2022. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract.. IEEE Access, pp. 1-1, https://doi.org/10.1109/ACCESS.2021.3140091..

Lajam, A. & Helmy., A., 2021. Performance evaluation of IPFS in private networks,. 4th International Conference on Data Storage and Data Engineering [Preprint]., pp. 1-1, Doi:10.1145/3456146.3456159..

Land, E. H., 1986. Recent advances in Retinex theory. In: Vision research, 26(1), pp. 7-21.

Land, E. H. & McCann, J., 1971. Lightness and retinex theory. In: Journal of the Optical Society of America A, 61(1), pp. 1-11.

Lantada, A. D., 2020. Engineering Education 5.0: Continuously Evolving Engineering Education. International Journal of Engineering Education, (36)((6)), pp. 1814–1832,.

Laughlin, S., 1981. A simple coding procedure enhances a neuron's information capacity. Zeitschrift für Naturforschung c, 36(9-10), pp. 910-912.

Lee, C., Lee, C. & Kim, C., 2012. Contrast enhancement based on layered difference representation. 19th IEEE International Conference on Image Processing , pp. 965-968.

Lee, W. & Choi, Y., 2020. Vulnerability and cost analysis of heterogeneous smart contract programs in blockchain systems.. Current Trends in Computer Sciences & Applications, (2)((1)), pp. 1, https://doi.org/10.32474/ctcsa.2020.02.000126.

Lee, Z., Chua, R. L. H., Keoh, S. L. & Ohba., Y., 2019. Performance Evaluation of Big Data Processing at the Edge for IoT-Blockchain Applications. IEEE Global Communications Conference (GLOBECOM), pp. 1-6, doi: 10.1109/GLOBECOM38437.2019.9013329..

Li, F. a. L. K., 2022. Research on multi service collaboration mode of university smart library based on blockchain. Seventh International Conference on Cloud Computing and Big Data Analytics (ICCCBDA), pp. pp. 217-220.

Liu, A., Khatun, M. S., Liu, H. & Miraz., M. H., 2021. Lightweight Blockchain of Things (BCoT) Architecture for Enhanced Security: A Literature Review. International Conference on Computing, Networking, Telecommunications & Engineering Sciences Applications (CoNTESA), pp. 25-30, doi: 10.1109/CoNTESA52813.2021.9657112..

Liu, D., M, G. & SA., J., 2012. University of Queensland vital signs dataset: development of an accessible repository of anesthesia patient monitoring data for research.. Anesth Analg., pp. 114 (3):584-9, doi: 10.1213/ANE.0b013e318241f7c0.

Ll. Tobarra, S. R. R. H. R. P. M. C. A. Y. A.-Z. B. H. M. D. A. R.-G. a. A. C. C., 2015. Analysis of Integration of Remote Laboratories for Renewable Energy courses at Jordan Universities. IEEE Frontiers in Education Conference Proceedings, El Paso, Texas, USA.

Llanos Tobarra, S. R. R. P. R. H. M. C. A. A.-Z. M. D. A. R.-G. A. C. J. C., 2016. An Integrated Example of Laboratories as a Service into Learning Management Systems. International Journal of Online Engineering (iJOE), Vol. 12(No. 9), p. pp. 32–39.

Lucas, B. a. P. R., 2019. Consensus Algorithm for a Private Blockchain. 9th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), p. pp. 264–271.

Lunardi, R. C. M. R. A. N. C. V. &. Z. A. F., 2018. Distributed access control on IoT ledger-based architecture. IEEE/IFIP Network Operations and Management Symposium: Cognitive Management in a Cyber World. NOMS 2018, p. pp. 1–7..

Lu, W., Wu, L. & Xue, F., 2021. Blockchain Technology for Projects: A Multicriteria Decision Matrix.. Project Management Journal, pp. 84-99, https://doi.org/10.1177/87569728211061780..

Machotka, J., Nafalski, A. & Nedić, Z., 2011. The History of Developments of Remote Experiments. 2nd World Conference on Technology and Engineering Education (2011 WIETE),, pp. 1-1, http://www.wiete.com.au/conferences/2wctee/papers/17-12-Machotka-J.pdf.

Magnusson, S., 2018. Evaluation of Decentralized Alternatives to PKI for IoT Devices: A litterature study and proof of concept implementation to explore the viability of replacing PKI with decentralized alternatives.

Maini, R. & Aggarwal, H., 2010. A comprehensive review of image enhancement techniques.. s.l.:arXiv preprint arXiv:1003.4053..

Majumder, A. & Irani, S., 2006. Contrast enhancement of images using human contrast sensitivity. In Proceedings of the 3rd symposium on Applied perception in graphics and visualization, ACM , pp. 69-76.

Ma, K., Zeng, K. & Wang, Z., 2015. Perceptual quality assessment for multi-exposure image fusion. IEEE Transactions on Image Processing, 24(11), p. 3345–3356.

Maloney, T. L., 1986. Evaluation of linear models of surface spectral reflectance with small numbers of parameters. In: Journal of the Optical Society of America, 3(1), pp. 1673-1683.

Ma, N. et al., 2023. Blockchain + IoT sensor network to measure, evaluate and incentivize personal environmental accounting and efficient energy use in indoor spaces,. Applied Energy, (332)((0306-2619)), pp. 1-1, https://doi.org/10.1016/j.apenergy.2022.120443.

Marimont, D. H. & Wandell, B. A., 1992. Linear models of surface and illuminant spectra., vol. 3, pp. .. In: Journal of the Optical Society of America A, 3(1), pp. 1673-1683.

Markus, S. & Buijs., P., 2022. Beyond the hype: how blockchain affects supply chain performance.,. Supply Chain Management: An International Journal, pp. 177-193, https://doi.org/10.1108/SCM-03-2022-0109.

Marr, D. & Vision, A., 1982. A computational investigation into the human representation and processing of visual information.. San Francisco: WH San Francisco: Freeman and Company.

MAY, K., 2018. Blockchain Issues | #1: Data Storage, s.l.: s.n.

McCamy & S., C., 1992. Correlated colour temperature as an explicit function of chromaticity coordinates. In: Journal of Colour Research & Application, 17(2), pp. 142-144.

McCann, J., 1983. Method and apparatus for lightness imaging. United States, Patent No. 4384336.

Md.AshrafUddin, A. S. I. G. V., 2021. A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions. Blockchain: Research and Applications, Elsevier, pp. 1-80.

Melissari, F. et al., 2021. Experiences Using Ethereum and Quorum Blockchain Smart Contracts in Dairy Production. International journal of production research, pp. 5758-5770, https://doi.org/10.3390/jsan13010006.

Meyer, M. A. & Booker, J. M., 2001. Eliciting and Analysing Expert Judgement: A Practical Guide. SIAM edition, Philadelphia, Issue ISBN 0-89871-474-5..

Michael A. Peters, 2016. Technological Unemployment: Educating for the Fourth Industrial Revolution. Educational Philosophy and Theory, (49)((1)), pp. 1–6, https://doi.org/ 10.1080/00131857.2016.1177412.

Mishev, E. K. a. A., 2017. Blockchain solutions for big data challenges: A literature review. 17th International Conference on Smart Technologies (IEEE EUROCON 2017), pp. 763-768.

Mishra, N., Lin, C.-C. & Chang., H.-T., 2015. A cognitive adopted framework for IOT big-data management and Knowledge Discovery Prospective. International Journal of Distributed Sensor Networks, pp. 1–12, doi:10.1155/2015/718390..

Mohamad, K., Giuseppe, D., DeFranco, J. & prince., p., 2021. Blockchain-Engineers Wanted: an Empirical Analysis on Required Skills, Education and Experience.. pp. 1-1, DOI:10.1109/WETSEB52558.2021.00014..

Mohammed, B. & Hasan, D., 2023. Smart healthcare monitoring system using IoT. International Journal of Interactive Mobile Technologies (Ijim),, (17)((01)), pp. 141-152, https://doi.org/10.3991/ijim.v17i01.34675.

Moinet, A., Darties, B. & Baril, J., 2017. Blockchain Based Trust and Authentication for Decentralized Sensor Networks. arXiv preprint, pp. 1-1, arXiv:1706.01730.

Monaco, L., Vogt, D. & Fransson, T., 2012. Implementation of a Remote Pump Laboratory Exercise in the Training of Engineering Students.. Proceedings of the ASME Turbo Expo 2012: Turbine Technical Conference and Exposition., Volume Volume 3: Cycle Innovations; Education; Electric Power; Fans and Blowers; Industrial and Cogeneration., pp. 479-487, https://doi.org/10.1115/GT2012-69983..

Moosavi, J., Naeni, L., Fathollahi-Fard, A. & Fiore, U., 2021. Blockchain in supply chain management: a review, bibliometric, and network analysis.. Environmental Science and Pollution Research, pp. 1-15, https://doi.org/10.1007/s11356-021-13094-3..

Morais, A. M. d. et al., 2021. A Solution for Integrating Virtual Learning Environments with Blockchain. Research, Society and Devel-opment, (10)((12)), pp. 1-1, https://doi.org/10.33448/rsd-v10i12.20354.

Morel, J. M., Petro, A. B. & Sbert, C., 2010. A PDE formalization of retinex theory. In: IEEE Transactions on Image Processing, 19(11), pp. 2825-2837.

Moudoud, H., Cherkaoui, S. & Khoukhi., L., 2021. Towards a Scalable and Trustworthy Blockchain: IoT Use Case. ICC 2021 - IEEE International Conference on Communications,, pp. 1-6, doi: 10.1109/ICC42927.2021.9500535.

Mourtzis, D., Vlachou, E., Dimitrakopoulos, G. & Zogopoulos., V., 2018. Cyber-Physical Systems and Education 4.0: The Teaching Factory 4.0 Concept. Procedia Manufacturing, Volume (23), pp. 129–134, https://doi.org/10.1016/j.promfg.2018.04.005.

M, S., S, D., D, H. & E., H., 1998. A Bayesian approach to filtering junk e-mail.. Learning for Text Categorization: Papers from the 1998 workshop, Volume (62), p. 98–105.

Muradi, S. & Chiam, Y., 2022. Identification of selection criteria for blockchain platforms. International Conference on Frontiers of Communications, Information System and Data Science (CISDS), pp. 8-13, https://doi.org/10.1109/cisds57597.2022.00009.

Nakamoto., S., 2009. Bitcoin: A peer-to-peer electronic cash system,. pp. 1, Available: http://www.bitcoin.org/bitcoin.pdf.

Narasimhan, Ramesh, V. & Nayar, 2003. A class of photometric invariants: Separating material from shape and illumination.. In Proceedings Ninth IEEE International Conference on Computer Vision, pp. 1387-1394, https://doi.org/10.1109/ICCV.2003.1238652.

Ncube, N. D. & Terzoli., A., 2020. Private Blockchain Networks: A Solution for Data Privacy. 2nd International Multidisciplinary Information Technology and Engineering Con-ference (IMITEC), pp. 1–8, https://doi.org/10.1109/IMITEC50163.2020.9334132.

Nguyen, T., Nguyen, H. & Gia., T. N., 2024. Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications,. Journal of Network and Computer Applications,, (226)((1084-8045)), pp. 1-1, https://doi.org/10.1016/j.jnca.2024.103884.

Nishani, V. & Barkhi., R., 2021. Evaluating Blockchain Using COSO. Current Issues in Auditing, (15)((1)), pp. A57–A71, https://doi.org/10.2308/CIIA-2019-509.

Nissl, M., Sallinger, E., Schulte, S. & Borkowski, M., 2020. Towards Cross-Blockchain Smart Contracts.. arXiv (Cornell University), pp. 1, https://doi.org/10.48550/arxiv.2010.07352..

Nuss, M., Puchta, A. & Kunz, M., 2018. Towards blockchain-based identity and access management for Internet of Things in enterprises,. Trust, Privacy and Security in Digital Business, pp. 167–181, doi:10.1007/978-3-319-98385-1_12..

O. Novo, 2018. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE Internet of Things Journal,, Volume vol. 5, no. 2, pp. pp. 1184-1195.

Olorunsogo, T. O., 2024. INTEGRATING IOT IN PEDIATRIC HEALTHCARE: A SYSTEMATIC REVIEW OF CURRENT APPLICATIONS AND FUTURE DIRECTIONS FOR PANCREATIC DISEASES AND OBESITY. International medical science research journal (Print), (4)((3)), pp. 305–318, https://doi.org/10.51594/imsrj.v4i3.923.

Ortiz, S. H. C., Chiu, T. & Fox, M. D., 2012. Ultrasound image enhancement: A review. Biomedical Signal Processing and Control, 7(5), pp. 419-428.

Ouaddah, A. A. E. A. a. A. O. A., 2016. FairAccess: a new Blockchain-based access control framework for the Internet of Things.. Security Comm. Networks, p. 5943–5964..

Ozpinar, A. & Kalinyazgan, K., 2024. EMPOWERING EDUCATION THROUGH BLOCKCHAIN: THE K12NET ECOSYSTEM FOR SMART CONTRACTS AND EDUCATIONAL ASSETS.. Cambridge Open Engage, pp. 1, doi:10.33774/coe-2024-4pbg9.

Panagiotidis., P., 2022. Blockchain in education-the case of language learning,. European Journal of Education, (5)((1)), pp. 66–83, https://doi.org/10.26417/443gjm83.

Panagiotidis, P., 2022. Blockchain in education - the case of language learning. European Journal of Education, (5)((1)), pp. 66–83, https://doi.org/10.26417/443gjm83.

Pandey, G., Sahu, G. & Singh., M., 2023. Improving Data Integrity of IPFS On-Chain Proof,. 2023 6th International Conference on Contemporary Computing and Informatics (IC3I),, pp. 171-177, Doi: 10.1109/IC3I59117.2023.10398081..

Park, C., Barlongo, I. & Kim., Y., 2019. A Market Place Solution for Energy Trans- action on Ethereum Blockchain. IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 1–5, https://doi.org/10.1109/ IEMCON.2019.8936157.

Parkkinen, J. P., Hallikainen, J. & Jaaskelainen, T., 1989. Characteristic spectra of Munsell colors. In: Journal of the Optical Society of America A, 6(2), pp. 318-322.

Pattanaik, S. et al., 1998. A multiscale model of adaptation and spatial vision for realistic image display. In Proceedings of the 25th annual conference on Computer graphics and interactive techniques.

Pattanaik, S. N., Ferwerda, J. A., Fairchild, M. D. & Greenberg, D. P., 1998. A multiscale model of adaptation and spatial vision for realistic image display. In: Proceedings of the 25th annual conference on Computer graphics and interactive techniques, pp. 287-298.

Peters, M. A., n.d. Technological Unemployment: Educating for the Fourth Industrial Revolution. Educational Philosophy and Theory, Vol.49(1), pp. 1-6.

Petro, A., Sbert, C. & Morel, J., 2014. Multiscale retinex. Image Processing On Line, pp. 71-88.

Philip, J. et al., 2023. Smart Health Monitoring Using Deep Learning and Artificial Intelligence.. Revue d'intelligence artificielle,, (37)((2)), pp. 451–464, https://doi.org/10.18280/ria.370222.

Podolskiy, D., 2024. HiveMQ now delivers 80% higher MQTT throughput, HiveMQ.. pp. 1-1, Available at: https://www.hivemq.com/blog/hivemq-4-18-delivers-higher-mqtt-throughput/#heading-improving-intra-cluster-messaging-to-boost-throughput.

Popenici, S. & Kerr, S., 2017. Exploring the impact of artificial intelligence on teaching and learning in higher education. Research and Practice in Technology Enhanced Learning, pp. 1-1, https://doi.org/10.1186/s41039-017-0062-8.

Quayson, M., Avornu, E. & Bediako, A., 2024. Modeling the enablers of blockchain technology implementation for information management in healthcare supply chains. Modern Supply Chain Research and Applications, (6)((2)), pp. 101-121, https://doi.org/10.1108/MSCRA-06-2023-0028.

Rahman, A. et al., 2024. Machine learning and deep learning-based approach in smart healthcare: Recent advances, applications, challenges and opportunities.. AIMS Public Health., pp. 85-109, doi: 10.3934/publichealth.2024004..

Rahman, M. A. et al., 2018. A review on brightness preserving contrast enhancement methods for digital image. In Ninth International Conference on Graphic and Image Processing (ICGIP 2017), Volume 10615, p. 106152S.

Rahma, Z., X. Y., Khalil, I. & Kelarev., A., 2021. Blockchain for IoT: A critical analysis concerning performance and scalability,. Lecture Notes of the Institute for Computer Sciences, Social Informatics, and Telecommunications Engineering,, pp. 57–74, doi:10.1007/978-3-030-91424-0_4.

Ramesh, V. K. C., May 2019. Storing IoT Data Securely in A Private Ethereum Blockchain. Master Thesis, University of Nevada, Las Vegas.

Ramesh, V., Kim, Y. & Jo, J. Y., 2020. Secure IoT Data Management in a Private Ethereum Blockchain. IEEE 44th Annual Computers, Software, and Applications Conference (COM-PSAC), pp. 369–375, https://doi.org/10.1109/COMPSAC48688.2020.0-219.

Rani, P. S. et al., 2023. A Decentralized and Cooperative Methodology For Organ Donation Management Based on Ethereum Blockchain.. Journal of Cognitive Human-Computer Interaction., pp. 1-1, https://doi.org/10.54216/jchci.060101.

Rathore, H. M. A. G. M., 2020. A Survey of Blockchain Enabled Cyber-Physical Systems.. Sensors.

Rathore, H., Mohamed, A. & Guizani., M., 2020. A Survey of Blockchain Enabled Cyber-Physical Systems. Sensors, (20)((1)), pp. 282-310, https://doi.org/10.3390/s20010282.

Raza, Z., Haq, I. & Muneeb, M., 2023. Agri-4-all: a framework for blockchain based agricultural food supply chains in the era of fourth industrial revolution.. IEEE Access, Volume (11), pp. 29851-29867, https://doi.org/10.1109/access.2023.3259962.

Reddy, A. A. et al., 2013. Comparison of image enhancement techniques using retinex models. In: International Journal of Advanced Computer Engineering and Communication Technology, 2(3), pp. 7-12.

Reis-Marques, Reis-Marques, C., Figueiredo, R. & Neto, M. d. C., 2021. Applications of Blockchain Technology to Higher Education Arena: A Bibliometric Analysis. European Journal of Investigation in Health, Psychology and Education, (1)1((4)), pp. 1406–1421, https://doi.org/10.3390/e, ji-hpe11040101.

Ren, Y., Ying, Z., Li, T. & Li, G., 2018 . LECARM: low-light image enhancement using the camera response model. IEEE Transactions on Circuits and Systems for Video Technology, 29(4), pp. 968-981.

Reyna, A. C. M. J. C. E. S. a. M. l., 2018. On blockchain and its integration with IoT: challenges and opportunities. Future Generation Computer Systems, Volume vol. 88, pp. pp. 173-190.

Reyna, A. et al., 2018. On blockchain and its integration with IoT: challenges and opportunities. Future Generation Computer Systems, Volume (88), pp. 173- 190, https://doi.org/10.1016/j.future.2018.05.046.

Reyna, A. et al., 2019. On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, pp. 173-190, Doi:10.1016/j.future.2018.05.046.

Rodrigues, C. K. D. S. & Rocha., V., 2021. Towards Blockchain for Suitable Efficiency and Data Integrity of IoT Ecosystem Transactions. IEEE Latin America Transactions, (19)((7)), pp. 1199–1206, https://doi.org/10.1109/TLA.2021.9461849.

Rossum, M. V. et al., 2022. Adaptive threshold-based alarm strategies for continuous vital signs monitoring. J Clin Monit Comput.. pp. 407-417, doi: 10.1007/s10877-021-00666-4.

Rostam., H., Motameni, H. & Enayatifar., R., 2023. Privacy-preserving in the smart healthcare system using steganography and chaotic functions based on DNA.. Security and privacy,, (7)((3)), pp. 1, https://doi.org/10.1002/spy2.363..

Routray, S. & Ganiga., R., 2021. Secure Storage of Electronic Medical Records (EMR) on Interplanetary File System (IPFS) Using Cloud Storage and Blockchain Ecosystem,.

Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1-9, Doi: 10.1109/ICECCT52121.2021.9616690..

Rožman, N. et al., 2022. Scalability Solutions in Blockchain-Supported Manufacturing: A Survey.. Strojniški Vestnik - Journal of Mechanical Engineering,, (68)((10)), pp. 585–609, https://doi.org/10.5545/sv-jme.2022.355.

Rundo, L. et al., 2019. MedGA: a novel evolutionary method for image enhancement in medical imaging systems.. Expert Systems with Applications, Volume 119, pp. 387-399.

Saba, T. et al., 2018. Image enhancement and segmentation techniques for detection of knee joint diseases: A survey.. Current Medical Imaging Reviews, 14(5), pp. 704-715.

Sabrina, F., Li, N. & Sohail, S., 2022. A Blockchain-Based Secure IoT System Using Device Identity Management. Sensors.

Sadawi, A. A., Hassan, M. S. & M. Ndiaye, 2021. A Survey on the Integration of Blockchain with IoT to Enhance Performance and Eliminate Challenges,. IEEE Access, Volume Vol. 9, pp. 54478-54497, doi: 10.1109/ACCESS.2021.3070555..

Sadawi, A. A. et al., 2020. A Hierarchical Blockchain of Things Network For Unified Carbon Emission Trading (HBUETS): A Conceptual Framework,. IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD), pp. 1-7, doi: 10.1109/ICTMOD49425.2020.9380610.

Sahonero-Alvarez, G., 2018. Blockchain and Peace Engineering and its Relationship to Engineering Education. World Engineering Education Forum-Global Engineering Deans Council (WEEF-GEDC), pp. 1-6, https://doi.org/10.1109/WEEF-GEDC.2018.8629679.

Saichandana, B., Ramesh, S., Srinivas, K. & Kirankumar, R., 2014. Image fusion technique for remote sensing image enhancement. In ICT and Critical Infrastructure Proceedings of the 48th Annual Convention of Computer Society of India, Volume II , pp. 235-242.

Saini, A. et al., 2021. A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System. IEEE Internet of Things Journal, (8)((7)), pp. 5914–5925, https://doi.org/10.1109/JIOT.2020.3032997.

Salmon, G., 2019. May the Fourth be with you: Creating Education 4.0. Journal of Learning for Development, (6)((2)), pp. 95-115, https://jl4d.org/index.php/ejl4d/article/view/352.

Sanka, A. a. C., 2021. A systematic review of blockchain scalability: Issues, solutions, analysis and Future Research. Journal of Network and Computer Applications, p. p. 103232..

Sapiro, G., 1999. Colour and illuminant voting. IEEE Transaction on Pattern Analysis and Machine Intelligence, 21(11), pp. 1210-1215.

Sarage, G. & Jambhorkar, S., 2011. Enhancement of Mammography Images for Breast Cancer Detection using Histogram Processing Techniques 1.

Sarica, A., Cerasa, A. & Quattrone, A., 2017. Random Forest Algorithm for the Classification of Neuroimaging Data in Alzheimer's Disease: A Systematic Review.. Frontiers in Aging Neuroscience, pp. 1-1, https://doi.org/10.3389/fnagi.2017.00329..

Saunders, M., Lewis, P. & Thornhill., A., 2003. Research methods forbusiness students. Essex: Prentice Hall: Financial Times.

Schäffer, M., di Angelo, M. & Salzer, G., 2019. Performance and scalability of private Ethereum blockchains,. Business Process Management: Blockchain and Central and Eastern Europe Forum,, pp. 103–118, doi:10.1007/978-3-030-30429-4_8..

Scheid, E. et al., 2022. On the Employment of Machine Learning in the Blockchain Selection Process. IEEE Transactions on Network and Service Management, pp. 3835-3846, https://doi.org/10.1109/TNSM.2022.3212917..

Schmidgen., H., 2021. The Laboratory. Encyclopedia of the History of Science,, pp. 1-1, https://doi.org/10.34758/sz06-t975.

Schwab, K., 2016. The Fourth Industrial Revolution. New York: Crown Publishing.

Scornet, E., G., B. & Vert, J., 2014. Consistency of Random Forests.. Annals of Statistics, pp. 1716-1741, https://doi.org/10.1214/15-AOS1321..

Sedky, M., Moniri, M. & Chibelushi, C. C., 2014. Spectral-360: A Physics-Based Technique for Change Detection. In: IEEE Conference In Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 405-408.

Serada, A., Sihvonen, T. & Harviainen, J., 2021. CryptoKitties and the new ludic economy: how blockchain introduces value, ownership, and scarcity in digital gaming.. Games and Culture, 16(4)), pp. 457-480.

Shahbazi, Z. a. B. Y., 2021. Integration of blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing. Sensors, Volume vol. 21(4), pp. pp. 1-21.

Shahbazi, Z. & Byun, Y., 2021. Integration of blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing. Sensors, Volume (21), pp. 1-21, https://doi.org/10.3390/s21041467..

Shammar, E., Zahary, A. T. & Al-Shargabi., A. A., 2021. A Survey of IoT and Blockchain Integration: Security Perspective. IEEE Access, Volume (9), pp. 156114–156150, https://doi.org/10.1109/ACCESS.2021.3129697.

Sharma., S., Sharma, T., Tiwari, A. & Gupta., S., 2024. Streamlining IoT-driven Data Using Blockchain.. Int Res J Adv Engg Mgt, pp. 1509–1514, https://doi.org/10.47392/irjaem.2024.0204.

Sharma, N. & Rohilla, R., 2024. Scalable and cost-efficient POA consensus-based blockchain solution for vaccination record management. Wireless Personal Communications, (135)((2)), pp. 1177–1207, doi:10.1007/s11277-024-11115-1..

Sharma, P., Chen, M.-Y. & Park., J. H., 2018. A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. IEEE Access, Volume (6), pp. 115–124, https://doi.org/10.1109/ACCESS.2017.2757955.

Shava., E. & Mhlanga., D., 2023. Mitigating bureaucratic inefficiencies through blockchain technology in Africa. Front. Blockchain 6:1053555., Volume (6), pp. 1, doi: 10.3389/fbloc.2023.1053555.

Shen, J., 2003. On the foundations of vision modeling: I. Weber's law and Weberized TV restoration.. Physica D: Nonlinear Phenomena, 175(175), pp. 241-251.

Shen, J., Li, Y., Zhou, Y. & Wang., X., 2019. Understanding I/O performance of IPFS storage: A client's perspective,. IEEE/ACM 27th International Symposium on Quality of Service (IWQoS),, p. 1–10.

Shin, H., Lee, M. & Kim., S., 2023. Space and Cost-Efficient Reed-Solomon Code based Distributed Storage Mechanism for IPFS. 14th International Conference on Information and Communication Technology Convergence (ICTC), pp. 1165-1169, Doi: 10.1109/ICTC58733.2023.10392473.

Shin, Y. & Jeon, S., 2024. MQTree: Secure OTA Protocol Using MQTT and MerkleTree.. Sensors, [online], (24)((5)), pp. 1447, https://doi.org/10.3390/s24051447.

Sinclair, C., L, P. & S., M., 1999. An application of machine learning to network intrusion detection.. Computer Security Applications Conference, 1999. (ACSAC'99) Proceedings. 15th Annual, p. 371–7.

Singh, S. K., Jeong, Y.-S. & Park, J. H., 2020. A deep learning-based IoT-oriented infrastructure for secure smart City. Sustainable Cities and Society, (60)(ISSN 2210-6707,), pp. 1-1, https://doi.org/10.1016/j.scs.2020.102252.

Sivasankari, K. & Sathyamithran, V. S., 2022. IPFS Enabled Robust Mechanism for File Storage and Retrieval Using Block Chain,. Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), pp. 01-05, Doi: 10.1109/ICERECT56837.2022.10059644..

Son, D. H. et al., 2021. An Effective Frame-work of Private Ethereum Blockchain Networks for Smart Grid.,. International Con-ference on Advanced Technologies for Communications (ATC), pp. 312–317, https://doi.org/10.1109/ATC52653.2021.9598199.

Steiu, M., 2020. Blockchain in education–opportunities, applications, and challenges. First Monday, (25)((9)), pp. 1-33, Doi: 10.5210/fm.v25i9.10654.

Stitini, O. O. F. R. S. K. S. &. B. O., 2024. Combining IoMT and XAI for Enhanced Triage Optimization: An MQTT Broker Approach with Contextual Recommendations for Improved Patient Priority Management in Healthcare.. International Journal of Online and Biomedical Engineering (iJOE), p. pp. 145–162.

Subramanyam, B., Joshi, P., Meena, M. & Prakash, S., 2016. Quality based classification of images for illumination invariant face recognition. IEEE International Conference on Identity, Security and Behavior Analysis (ISBA) (pp.), pp. 1-6.

Su, C. a. X. L., 2021. A Review of Blockchain Consensus. International Conference on Intelligent Computing, Automation and Applications (ICAA), p. pp. 598–604.

Sukharev, P. a. S. D., 2018. Asynchronous Mining of Ethereum Cryptocurrency. IEEE International Conference on Quality Management, Transport and Information Security, Information Technologies, p. pp. 731–735.

Tantidham, T. & Aung, Y. N., 2019. Emergency Service for Smart Home System Using Ethereum Blockchain: System and Architecture. IEEE International Conference on Pervasive Com- puting and Communications Workshops (PerCom Workshops), pp. 888–893, https:// doi.org/10.1109/PERCOMW.2019.8730816.

Tanwar, S., Parekh, K. & Evans, R., 2020. Blockchain-based electronic healthcare record system for healthcare 4.0 applications.. Journal of Information Security and Applications, pp. 1, https://doi.org/10.1016/j.jisa.2019.102407..

Thakur, P. & Sehgal., V. K., 2024. Synergizing edge computing and blockchain for cyber-physical systems.. Concurrency and computation, (36)((12)), pp. 1, https://doi.org/10.1002/cpe.8066.

Thomas Hepp, M. S. P. E. A. S. a. B. G., 2018. On-chain vs. off-chain storage for supply-and blockchain integration. Information Technology, pp. 283-291.

Tian, M. & Chen, J., 2022. Smart contract in blockchain.,. Proceedings of the 2022 International Conference on Bigdata Blockchain and Economy Management (ICBBEM 2022), pp. 868-875, https://doi.org/10.2991/978-94-6463-030-5_86.

Tiruvayipati., S. et al., 2024. Methodology for Developing an IoT-based Parking Space Counter System using XNO.. Scalable Computing. Practice and Experience,, (25)((2)), pp. 800–811, https://doi.org/10.12694/scpe.v25i2.2459.

Tobarra, L. et al., 2015. Analysis of Integration of Remote Laboratories for Renewable Energy Courses at Jordan Universities. IEEE Frontiers in Edu-cation Conference (FIE), pp. 1–5, https://doi.org/10.1109/FIE.2015.7344388.

Tobarra, L. et al., 2016. Laboratories as a Service Integrated into Learning Management Systems. 13th International Conference on Remote Engineering and Virtual Instrumentation (REV), pp. 1-1, https://doi.org/10.1109/REV.2016.7444447.

Tottleben, A. V., Ihle, C., Schubotz, M. & Gipp., B., 2021. Academic Storage Cluster,. ACM/IEEE Joint Conference on Digital Libraries (JCDL), pp. 278-279, Doi: 10.1109/JCDL52503.2021.00034..

Tuli, S. M. R. T. S. &. B. R., 2018. FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing. Journal of Systems and Software.

Valliammal, N. & Geethalakshmi, S. N., 2011. A hybrid method for enhancement of plant leaf recognition. World of Computer Science and Information Technology Journal, 1(9), pp. 370-375.

Vargas, S. P. R. & Lindín, C., 2019. Blockchain in the University: Digital Technology to Design, Implement and Manage Global Learning Itineraries. Digital Education Review, Issue (35), pp. 130-150, http://dx.doi.org/10.1344/der.2019.35.130-150.

Venkatesh, S. K., Sarada, C., Vasavi, M. & Ambika., K., 2024. Securing IoT Devices from DDoS Attacks through Blockchain and Multi-Code Trust Framework.. E3S web of conferences,, Volume (472), pp. 03001–03001, https://doi.org/10.1051/e3sconf/202447203001.

Wadhwa, S. S. R. K. S. V. J. S. a. M. W. 2., 2022. Energy Efficient Consensus Approach of Blockchain for IoT Networks with Edge Computing. Sensors 22, Issue No. 10: 3733..

Wang, S. & L., G., 2017. Naturalness preserved enhancement algorithm using a priori multi-layer lightness statistics. IEEE Transactions on Image Processing, 27(2), pp. 938-948.

Wang, S. et al., 2015. A patch-structure representation method for quality assessment of contrast changed images. IEEE Signal Processing Letters, 22(12), pp. 2387-2390..

Wang, S., Zheng, J., Hu, H. & Li, B., 2013. Naturalness preserved enhancement algorithm for non-uniform illumination images. IEEE Transactions on Image Processing, 22(9), pp. 3538-354.

Wang, S. Z. J. H. H. a. L. B., 2013. Naturalness preserved enhancement algorithm for non-uniform illumination images. IEEE Transactions on Image Processing, 22(9), pp. 3538-3548.

Wark, M. A. a. N., 2019. Learning for Sustainable Development in the Fourth Industrial Revolution. Commonwealth of Learning, Volume 9.

Watson, A. B. & Solomon, J. A., 1997. Model of Visual Contrast Gain Control and Pattern Masking. In: Journal of the Optical Society of America A, 14(9), pp. 2379-2391.

Wenhua, Z. et al., 2023. Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. Electronics 12, Issue (3), pp. 1-1, https://doi.org/10.3390/electronics12030546..

Werner, E., Matias, J. C., Berejuck, M. D. & Saliah-Hassane., H., 2021. Evaluation of Blockchain Techniques to Ensure Secure Access on Remote FPGA Laboratories,. 9th International Symposium on Digital Forensics and Security (ISDFS), pp. 1–6, https://doi.org/10.1109/ISDFS52919.2021.9486318.

Whittle, P., 1986. Increments and decrements: luminance discrimination. Vision research, 26(10), pp. 1677-1691.

Windley, P., 2015. IBM's ADEPT Project: Rebooting the Internet of Things. pp. 1-1,https://www.windley.com/archives/2015/02/ibms_adept_project_rebooting_the_internet_of_things.shtml.

Wolfschmid., G., 2002. The Observatories and Instruments of Tycho Brahe. Analytica Chimica Acta, Volume (16), p. 203–216.

Wuttke, H. et al., 2019. The Remote Experimentation as the Practical-Oriented Basis of Inclusive Engineering Education. Int. J. Online Biomed. Eng.,, Volume Vol.15, pp. 4-17, https://doi.org/10.3991/IJOE.V15I05.9752..

Xiaochen Zheng, R. R. M. R. V. a. J. O.-M., 2018. Blockchain-based personal health data sharing system using cloud storage. IEEE 20th International Conference on e-Health Networking, Applications and Services, pp. 1-6.

Xiao, K. et al., 2020. Edge- ABC: An Architecture for Task Offloading and Resource Allocation in the Internet of Things. Future Generation Computer System, Volume (107), pp. 498–508, https://doi. org/10.1016/j.future.2020.02.026.

Xiwei Xu, I. W. M. S. L. Z. J. B. L. B. C. P. a. P. R., n.d. A taxonomy of blockchain-based systems for architecture design. IEEE International Conference on Software Architecture, Volume 2017, pp. 243-252.

Xue, H. et al., 2022. Integration of Blockchain and Edge Computing in Internet of Things: A Survey. arXiv (Cornell University), pp. 1-1, https://doi.org/10.48550/arxiv.2205.13160..

Xu, L. D. H. W. &. L. S., 2018. Internet of things in industries: A survey. IEEE Transactions on Industrial Informatics, Volume vol. 10(4), p. pp. 2233–2243.

Xu, L. D., Xu, E. L. & Li., L., 2018. Industry 4.0: State of the Art and Future Trends. International Journal of Production Research, (56)((8)), pp. 2941–2962, https://doi.org/10.1080/00207543.2018.1444806.

Xu, Q., Song, Z., Goh, R. S. M. & Li., Y., 2018. Building an Ethereum and IPFS-Based Decentralized Social Network System,. IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS),, pp. 1-6, Doi: 10.1109/PADSW.2018.8645058..

Y. Huang, B. W. a. Y. W., 2020. Research on Ethereum Private Blockchain Multi-nodes Platform. International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), p. pp. 369–372.

Yadav, A. K. & Vishwakarma, V. P., 2022. Adaptation of Blockchain of Things (BCOT): Opportunities and Challenges. 2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), pp. 1-5, doi: 10.1109/ICBDS53701.2022.9935985..

Zet, C. & Dumitriu., G.-C., 2021. Using Blockchain Technology for Ensuring Students Results Traceability for Instrumentation Classes. Measurement: Sensors, Volume (18), pp. 1-1, https://doi.org/10.1016/j.measen.2021.100315.

Zhang, C., Zhou, G., Li, H. & Cao., Y., 2020. Manufacturing Blockchain of Things for the Configuration of a Data- and Knowledge-Driven Digital Twin Manufacturing Cell. IEEE Internet of Things Journal, (7)((12)), pp. 11884-11894, doi: 10.1109/JIOT.2020.3005729..

Zhang, Z. et al., 2020. Industrial Blockchain of Things: A Solution for Trustless Industrial Data Sharing and Beyond. IEEE 16th International Conference on Automation Science and Engineering (CASE), pp. 1187-1192, doi: 10.1109/CASE48305.2020.9216817.

Zhaofeng, M., Lingyun, W., Xiaochang, W. & W. Zhen, Z. W., 2020. Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data. IEEE Internet of Things Journal, (7)((5)), pp. 4000-4015, doi: 10.1109/JIOT.2019.2960526..

Zhaofeng, M. et al., 2020. Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data. IEEE Internet of Things Journal, May, (7)((5)), pp. 4000-4015, doi: 10.1109/JIOT.2019.2960526..

Zhao, W. et al., 2021. Block-chain-Enabled Cyber–Physical Systems: A Review. IEEE Internet of Things Journal, (8)((6)), pp. 4023-4034, https://doi.org/10.1109/JIOT.2020.3014864..

Zhao, Y. et al., 2023. A Lightweight Model-Based Evolutionary Consensus Protocol in Blockchain as a Service for IoT. IEEE Transactions on Services Computing,, (16)((04)), pp. 2343-2358.

Zheng, Q., Li, Y., Chen, P. & Dong., X., 2018. An Innovative IPFS-Based Storage Model for Blockchain,. IEEE/WIC/ACM International Conference on Web Intelligence (WI), pp. 704-708, doi: 10.1109/WI.2018.000-8..

Zheng, S., Han, T., Jiang, Y. & Ge, X., 2020. Smart contract-based spectrum sharing transactions for multi-operators wireless communication networks.. IEEE Access, Volume (8), pp. 88547-88557, https://doi.org/10.1109/access.2020.2992385.

Zheng, X., Lu, J., Sun, S. & Kiritsis., D., 2020. Decentralized industrial IoT data management based on blockchain and IPFS. IFIP International Conference on Advances in Production Management Systems, Volume (Cham), pp. 222-229, https://doi.org/10.1007/978-3-030-57997-5_26.

Zhou, Y. et al., 2022. Application of Distributed Ledger Technology in Distribution Networks.. Proceedings of the IEEE, pp. 1963-1975, https://doi.org/10.1109/JPROC.2022.3181528..

Zhou, Z. et al., 2024. Blockchain-based secure and efficient secret image sharing with outsourcing computation in wireless networks.. IEEE Transactions on Wireless Communications,, (23)((1)), pp. 423-435 , https://doi.org/10.1109/twc.2023.3278108.

Zhuang., J., Fan., H. & Li., X., 2023. Research RSA accumulator-based stateless blockchain optimisation for smart contracts. Proc. SPIE 12718, International Conference on Cyber Security, Artificial Intelligence, and Digital Economy (CSAIDE 2023), pp. 1, https://doi.org/10.1117/12.2681597.

Zoican, S. M. V. R. Z. a. D. G., 2018. Blockchain and Consensus Algorithms in Internet of Things. International Symposium on Electronics and Telecommunications (ISETC), p. pp. 1–4.

Zubaydi, H., Varga, P. & Molnár, S., 2023. Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review.. Sensors, pp. 1-1, https://doi.org/10.3390/s23020788.

Appendix A

The source code used in this thesis is available on GitHub. It contains all scripts, data processing tools, and relevant documentation needed to reproduce the experiments and results discussed in this work. The repository is publicly accessible and can be found at the following link:

GitHub Repository: Thesis Code