USEFULNESS, AWARENESS, AND ADOPTABILITY OF IoT DEVICES USING BLOCKCHAIN TECHNOLOGY

By

EDIDIONG BASSEY BASSEY

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

July 2024

FSKTM 2024 17

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

USEFULNESS, AWARENESS, AND ADOPTABILITY OF IoT DEVICES USING BLOCKCHAIN TECHNOLOGY

By

EDIDIONG BASSEY BASSEY

July 2024

Chairman : Associate Professor Ts Rodziah binti Atan, PhD
Faculty : Computer Science and Information Technology

Traditionally, the high flexibility and scalability of cloud computing has made it a preferred choice for enabling on-demand resource sharing. Yet, the real-time requirements for data storage, data processing, and data interchange have increased dramatically with the rapid expansion of Internet of Things (IoT) in recent years, considerably exceeding the carrying capacity of traditional cloud computing. Specifically, high latency and bandwidth pressure impede the development of traditional cloud computing in IoT in many application scenarios, such as smart home devices, due to massive scale data transfer between billions of devices and data centres. In this regard, this study aims to associate data management in the IoT via edge computing using blockchain technology for technology-based companies.

A quantitative research method was taken for this research methodology. In order to obtain necessary data, questionnaires were sent out through Google form, focusing on employing a purposive random sampling strategy. The survey method was selected because it enables respondents to answer questions at their own leisure, cost-effective,

and able to gather a great quantity of data in a short period of time. The survey includes feedback from a total of 349 individuals working for 25 technology-based companies in Malaysia. For the purpose of conducting data analyses, the Statistical Package for Social Science (SPSS) version 26 was utilised as the statistical analysis tool.

Based on the research conducted in these technology-based companies, it has been found that the utilisation, awareness, and implementation of blockchain technology have a beneficial impact on the financial performance of data management in the Internet of Things (IoT) via edge computing. In addition, the blockchain utilisation, awareness and adoption model accounted for 50% of the observed variance in the dependent variable after controlling for all other factors.

Furthermore, the study findings suggest that blockchain utilisation, awareness and adoption presumed to be benefiting the traditional data service towards the proposed IoT data management implementation. According to the results, the technology-based companies may save up their expenses and enhance productivity output by adopting blockchain technology practices. The study shows that the existence of useful and impactful association link on the effect of blockchain usefulness, awareness and adoption approaches on internet of things data management with technology-based companies in Malaysia. The findings show that in order for technology-based companies to remain competitive, the management and the staff need to adopt blockchain technology practices.

The conclusions also suggest that technology-based companies should provide training to their staff on new techniques for creativity and encourage them to stay up to date with the latest innovations trends. The business success of technology-based companies can be improved with the help of good technologies adoption and efficiency of the teams towards the technology.

Keywords: Blockchain, Internet of Things, Edge Computing

SDG: GOAL 4: Quality Education, GOAL 11: Sustainable Cities and Communities

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

KAJIAN KE ATAS KEPENGGUNAAN, KESEDARAN, KEBOLEHGUNAAN PERANTI IOT MENGGUNAKAN BLOK RANTAI

Oleh

EDIDIONG BASSEY BASSEY

Julai 2024

Pengerusi : Profesor Madya Ts Rodziah binti Atan, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Secara tradisinya, pengkomputeran awan yang mempunyai fleksibiliti dan skalabiliti yang tinggi telah menjadikannya sebagai pilihan utama untuk membolehkan perkongsian sumber atas permintaan. Namun, keperluan masa nyata untuk penyimpanan data, pemprosesan data dan pertukaran data telah meningkat secara mendadak dengan perkembangan pesat Internet Benda (IoT) dalam beberapa tahun kebelakangan ini, yang melangkaui kapasiti bawaan pengkomputeran awan tradisional. Khususnya, kependaman tinggi dan tekanan lebar jalur menghalang pembangunan pengkomputeran awan tradisional IoT dalam banyak senario aplikasi, seperti peranti rumah pintar, disebabkan pemindahan data berskala besar antara berbilion peranti dan pusat data. Dalam hal ini, kajian ini bertujuan untuk mengaitkan pengurusan data IoT melalui pengkomputeran pinggir menggunakan teknologi blok rantai bagi syarikat berasaskan teknologi.

Kaedah kajian kuantitatif adalah metodologi bagi kajian ini. Untuk mendapatkan data yang diperlukan, soal selidik telah dihantar melalui borang Google, memfokus kepada

penggunaan strategi persampelan rawak bertujuan. Kaedah tinjauan ini dipilih kerana ia membolehkan responden menjawab soalan pada masa lapang mereka, menjimatkan kos, dan mampu mengumpulkan data pada kuantiti yang banyak dalam tempoh masa yang singkat. Tinjauan ini merangkumi maklum balas daripada 349 individu yang bekerja untuk 25 syarikat berasaskan teknologi di Malaysia. Bagi tujuan menjalankan analisis data, Pakej Statistik untuk Sains Sosial (SPSS) versi 26 digunakan sebagai alat analisis statistik.

Berdasarkan penyelidikan yang dijalankan ke atas syarikat berasaskan teknologi ini, didapati bahawa penggunaan, kesedaran, dan pelaksanaan teknologi blok rantai mempunyai kesan yang bermanfaat terhadap prestasi kewangan pengurusan data IoT melalui pengkomputeran pinggir. Sebagai tambahan, model penggunaan, kesedaran dan penggunaan blok rantai juga menyumbang sebanyak 50% daripada varians yang dikaji dalam pembolehubah bersandar selepas kawalan ke atas faktor lain dilaksanakan.

Selain itu, penemuan kajian mencadangkan bahawa penggunaan, kesedaran dan penggunaan blok rantai dijangka mampu memberi manfaat kepada perkhidmatan data tradisional ke arah pelaksanaan kaedah pengurusan data IoT yang dicadangkan. Berdasarkan keputusan, syarikat berasaskan teknologi dapat menjimatkan perbelanjaan mereka dan meningkatkan output produktiviti dengan mengguna pakai amalan teknologi blok rantai. Kajian menunjukkan kewujudan beberapa perkaitan kesatuan yang berguna dan memberi kesan ke atas penggunaan kebergunaan blok rantai, kesedaran dan pendekatan penerimaan dalam pengurusan data Internet Benda dengan syarikat berasaskan teknologi di Malaysia. Penemuan menunjukkan bahawa untuk memastikan syarikat berasaskan teknologi kekal berdaya saing, pihak pengurusan dan kakitangan perlu mengamalkan amalan teknologi blok rantai.

Kesimpulan juga mencadangkan bahawa syarikat berasaskan teknologi harus menyediakan latihan kepada kakitangan mereka berkaitan teknik baharu untuk kreativiti dan menggalakkan mereka untuk mengikuti perkembangan tren inovasi terkini. Kejayaan perniagaan syarikat berasaskan teknologi boleh dipertingkatkan dengan bantuan penggunaan teknologi dan kecekapan pasukan terhadap teknologi yang berkesan.

Kata Kunci: Blok Rantai, Internet Benda, Pengkomputeran Pinggir

SDG: MATLAMAT 4: Pendidikan Berkualiti, MATLAMAT 11: Bandar dan Masyarakat Mampan

ACKNOWLEDGEMENTS

At the outset, I would like to convey my profound appreciation and indebtedness to the God almighty, who bestowed upon me his blessings throughout the duration of my academic pursuit, enabling me to successfully conclude the research work and fulfil the requirements of my program.

I would like to utilise this opportunity to convey my sincerest gratitude and appreciation to my supervisor, Prof. Madya. Dr. Rodziah Binti Atan and co-supervisor Dr. Mohd Izuan Hafez Ninggal. I experienced a great sense of honour and pleasure while working and acquiring knowledge under the guidance of my supervisor and mentor during the period of my study. I am deeply appreciative of the extensive assistance that they have provided me with throughout the years.

Finally, I wish to convey my sincere appreciation to the faculty members and the wider academic community of Universiti Putra Malaysia for affording me the privilege to undertake this research project, and for providing the essential resources and guidance that have enabled me to accomplish it with success.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Rodziah binti Atan, PhD
Associate Professor, Ts
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Mohd Izuan Hafez bin Ninggal, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 13 March 2025

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

IoT	Internet of Things
DV	Dependent Variable
IVs	Independent Variables
UBT	Understanding of Blockchain Technology
ALE	Awareness Level Evaluation
YO	Your Opinion
MSA	Measure of Sampling Adequacy
SPSS	Statistical Package for Social Science

LIST OF SYMBOLS

α	Alpha
R^2	Coefficient of determination
β	Beta
%	Percentage
Sig	Significant Value
t	t-value

CHAPTER 1

INTRODUCTION

This chapter provides an overview of the study, presenting the problem statement as the basis for conducting the research. It outlines the research objectives, questions, hypotheses, significance, and scope, concluding with a summary of the chapter. Additionally, this chapter elaborates on the key concepts of the study, emphasizing the researcher’s focus and rationale for developing this research.

1.1 Research Background

The IoT has garnered significant attention from academics, researchers, and entrepreneurs due to its ability to offer innovative services across a wide range of applications (Dinh et al., 2019; Fatma et al., 2020; Muhammad et al., 2019). IoT integrates various devices into a physical network where sensing, processing, and communication operations are automated, eliminating the need for human intervention (Soumyashree et al., 2019).

With the rise of smart homes, smart cities, and other intelligent technologies, IoT is a rapidly growing field. By 2020, more than 50 billion connected devices were projected to exist (Minhaj et al., 2018). Several network technologies, including Wireless Sensor Networks (WSNs), Machine-to-Machine (M2M), and Cyber-Physical Systems (CPS), are fundamental components of IoT. However, security concerns arise with these technologies, particularly when they rely on standard IP network protocols, requiring robust security measures to protect against threats. Malicious attacks could compromise IoT services, risking data security, privacy, and confidentiality.

The integration of blockchain and IoT offers several benefits. Blockchain’s decentralized and distributed architecture addresses the security risks and single points of failure inherent in centralized IoT systems. Its use of cryptographic algorithms, hash functions, and timestamps provides enhanced security and privacy. Moreover, blockchain’s immutable ledger protects IoT data by requiring validation from a majority of participants before any data changes are made (Verma & Arora, 2022). This creates a trusted system in which IoT devices themselves approve or reject transactions based on consensus (Adhikari & Ramkumar, 2023).

Although blockchain was initially developed for cryptocurrencies, it holds great potential for securing IoT applications (Nils et al., 2020; Ali et al., 2023). By enabling decentralized, tamper-proof data storage and processing, blockchain enhances the security of IoT networks (Zubaydi et al., 2023). However, IoT systems can suffer from bottlenecks due to the vast amounts of data generated by devices, leading to degraded quality of service (Dutta et al., 2023). The peer-to-peer structure of blockchain is seen as a promising solution to this issue, addressing both data bottlenecks and eliminating single points of failure (Qiheng et al., 2020; Partha et al., 2020).

Blockchain also reduces the need for trust in centralized authorities or intermediaries by relying on a technological mechanism (Junqin et al. 2019; Zubaydi et al., 2023). Instead of placing trust in a third party, participants in a blockchain system place trust in the technology itself (Filippi et al., 2020). Open-source software and the transparency of blockchain protocols enhance trust in the system, as the outcomes of specific software can be predicted. For instance, the Bitcoin protocol, users can verify that miners will receive a predictable reward for creating new blocks without relying on any central authority (Andreas, 2020). This technological transparency reinforces trust among participants, ensuring that no single entity holds excessive power.

1.1.1 IoT with Blockchain

The IoT has emerged as one of the most groundbreaking technologies for connecting virtual and physical devices over the internet, opening up a slew of new possibilities in various fields. The unforeseen growth of the IoT system has opened up new opportunities in multiple areas. However, there are still several challenges with the IoT that act as a roadblock to the expected widespread adoption of IoT devices. The absence of trust and confidence is one of these concerns. In the present IoT centralised paradigm, a third-party central authority has complete control over data collecting and processing from multiple IoT objects, with no explicit constraints on utilising the data. As a result, the central authority acts as a block box for IoT users, which appeals to the majority of IoT device owners (Gugueoth et al., 2023). Table 1.1 compares IoT with blockchain in a straightforward manner.

Table 1.1 : A Simple Comparison between IoT and Blockchain

	Items	IoT	Blockchain
1	Privacy	Privacy is not guaranteed	Privacy is not guaranteed
2	Bandwidth	Limited bandwidth	Uncontrolled bandwidth
3	Structure	Centralised	Decentralised
4	Scalability	Scales well with many nodes	Scales poorly with many nodes
5	Resources	Controlled	Uncontrolled
6	Latency	Requires low latency	High time consumption
7	Security	Poor security capability	Robust security capability

On the other hand, blockchain technology creates a decentralised, autonomous, trustless, and distributed environment. In contrast to the centralised model, which has difficulties such as a single point of failure, trust, and security, the blockchain uses a decentralised approach to employ the processing powers of all contributing users, resulting in improved efficiency and the elimination of a single point of failure. Also, blockchain enhances data security and integrity due to its tamper-proof and immutability properties (Jnr et al., 2023). Each tech has similarities and differences.

1.2 Research Problem

The current IoT infrastructure in Malaysia is predominantly built on a centralized server-client model, where cloud servers handle device identification, verification, and communication. While this model has supported small-scale IoT networks, it is not sustainable as IoT ecosystems continue to grow. This centralized architecture incurs high costs for infrastructure and maintenance, as cloud servers, networking equipment, and data storage systems become more expensive with the increasing number of connected devices (Mangur, 2020). Moreover, the growing volume of data and communication generated by billions of IoT devices presents scalability challenges and potential points of failure (Maayan, 2020).

The reliance on central servers not only introduces bottlenecks but also poses a risk to network reliability, particularly for essential services tied to human life and health (Allioui & Mourdi, 2023). Additionally, the diversity in IoT device ownership and the lack of standardization among cloud services further complicate interoperability, leading to fragmented systems with limited compatibility. IoT infrastructure firms are increasingly recognizing the essential need to transition to the blockchain technology, driven by its potential for innovation and differentiation. By leveraging blockchain, developers can create distributed applications that operate without reliance on a centralized server. This capability enables the development of trustworthy applications that are subject to external scrutiny (Prasad et al., 2018).

Moreover, the integration of smart contracts—self-executing agreements coded directly onto the blockchain—further enhances operational efficiency. This automation allows many corporate processes to be streamlined, reducing the need for intermediaries and ultimately lowering costs (Khan et al., 2021). Additionally, blockchain technology contributes to improved data security, privacy, and management, all of which are critical elements in contemporary software engineering (Zou et al. 2019,). By understanding the perceived usefulness, awareness and adoption of a blockchain, IoT infrastructure firms can enhance their productivity, increase safety, and expand their market access, positioning themselves for greater success in a competitive landscape.

Despite blockchain successful implementation in various countries and sectors, blockchain technology remains in its early stages in Malaysia (Nazim et al., 2021). There is a notable lack of familiarity with blockchain among Malaysians, coupled with insufficient regulatory frameworks. However, there is growing interest in blockchain as global technological advancements unfold. Although local legislation is still developing, the Malaysian government has expressed openness to utilizing blockchain in sectors such as renewable energy, palm oil, and Islamic finance (Nazim et al., 2021). While blockchain has found applications in several domestic contexts, existing literature indicates that the software sector and its associated firms are not adequately focused on exploring this technology.

However, issues related to its usefulness, awareness, and adoption of Blockchain within the Malaysian IoT ecosystem remain underexplored. There is insufficient understanding of how blockchain can address the mentioned concerns of IoT networks. Furthermore, the awareness of blockchain's benefits and its potential adoption among Malaysian businesses and industries has not been thoroughly investigated.

1.3 Research Objective

The purpose of this study is to address key issues related to the usefulness, awareness, and adoption trends of Blockchain technology within Malaysia's IoT ecosystem, as outlined in the problem statements. By examining these focal points, the research provides a structured analysis of Blockchain's impact, potential, and acceptance within IoT applications. Consequently, the objectives of this study are as follows:

i. To assess the perceived usefulness of Blockchain technology within the IoT ecosystem in Malaysia.

ii. To evaluate the level of awareness and understanding of Blockchain technology among IoT developers in Malaysia.

iii. To assess the adoption rate of Blockchain technology in the Malaysian IoT ecosystem.

1.4 Research Question

This study aims to investigate specific issues concerning Blockchain's usefulness, awareness, and adoption within Malaysia's IoT ecosystem. To guide this inquiry, the following research questions are formulated:

i. How do IoT developers in Malaysia perceive the usefulness of Blockchain technology in addressing key challenges within IoT?

ii. What is the current level of awareness and understanding of Blockchain technology among IoT professionals in Malaysia?

iii. What are the current adoption trends of Blockchain technology within the Malaysian IoT ecosystem?

1.5 Research Hypothesis

This study seeks to explore the relationship between Blockchain technology and its perceived usefulness, awareness, and adoption within the IoT ecosystem in Malaysia. To guide this investigation, the following hypotheses are proposed based on the research objectives:

i. There is a positive relationship between the perceived usefulness of Blockchain technology and the IoT ecosystem in Malaysia

ii. There is a positive relationship between the awareness of Blockchain technology and the IoT ecosystem in Malaysia

iii. There is a positive relationship between the adoption rate of Blockchain technology and the IoT ecosystem in Malaysia

1.6 Research Significance

This study on the integration of Blockchain technology within the IoT ecosystem in Malaysia holds significant importance for multiple stakeholders.

Theoretical Contribution

This study contributes to the academic literature by addressing significant gaps in understanding the perceived usefulness, awareness, and adoption of Blockchain among IoT developers. By concentrating on these aspects, the research offers a comprehensive analysis of how Blockchain technology can improve security, privacy, and scalability within IoT applications. In doing so, it advances theoretical frameworks pertinent to emerging technologies, providing valuable insights into the interplay between Blockchain and the IoT ecosystem.

Practical Contributions

The findings of this study will have practical implications for businesses and organizations operating within the IoT sector. As industries increasingly acknowledge the significance of secure and efficient data management solutions, this research can assist companies in recognizing the potential advantages of Blockchain technology. By evaluating the existing levels of awareness and adoption trends, organizations can formulate targeted strategies to enhance their operations, thereby fostering increased competitiveness and innovation in the marketplace.

Policy Contribution

Policymakers and regulatory bodies can gain valuable insights from this study. By understanding the barriers to Blockchain adoption and the current landscape of IoT in Malaysia, they can make informed policy decisions that encourage technology integration, ensuring that regulations facilitate rather than impede technological advancement. In summary, this research not only enhances academic discourse but also provides critical insights for practitioners and policymakers, contributing to the broader conversation about the future of IoT and Blockchain in Malaysia.

1.7 Research Scope

The scope of this study is confined to examining Blockchain technology's usefulness, awareness, and adoption within Malaysia's IoT ecosystem. It targets 349 IoT developers and stakeholders across 25 ICT and IT industry players in Malaysia. Utilizing a quantitative methodology, the research employs Likert-scale surveys to gather data on perceptions and awareness levels. Quantitative data is analysed using statistical software (SPSS), with findings reflecting the past three years of IoT and Blockchain integration in Malaysia.

1.8 Research Activities Flow

The figure 1.1 outlines the key research activities for this study on the integration of Blockchain technology within the IoT ecosystem in Malaysia. This structured method guarantees a systematic study and analysis of the research hypotheses and objectives.

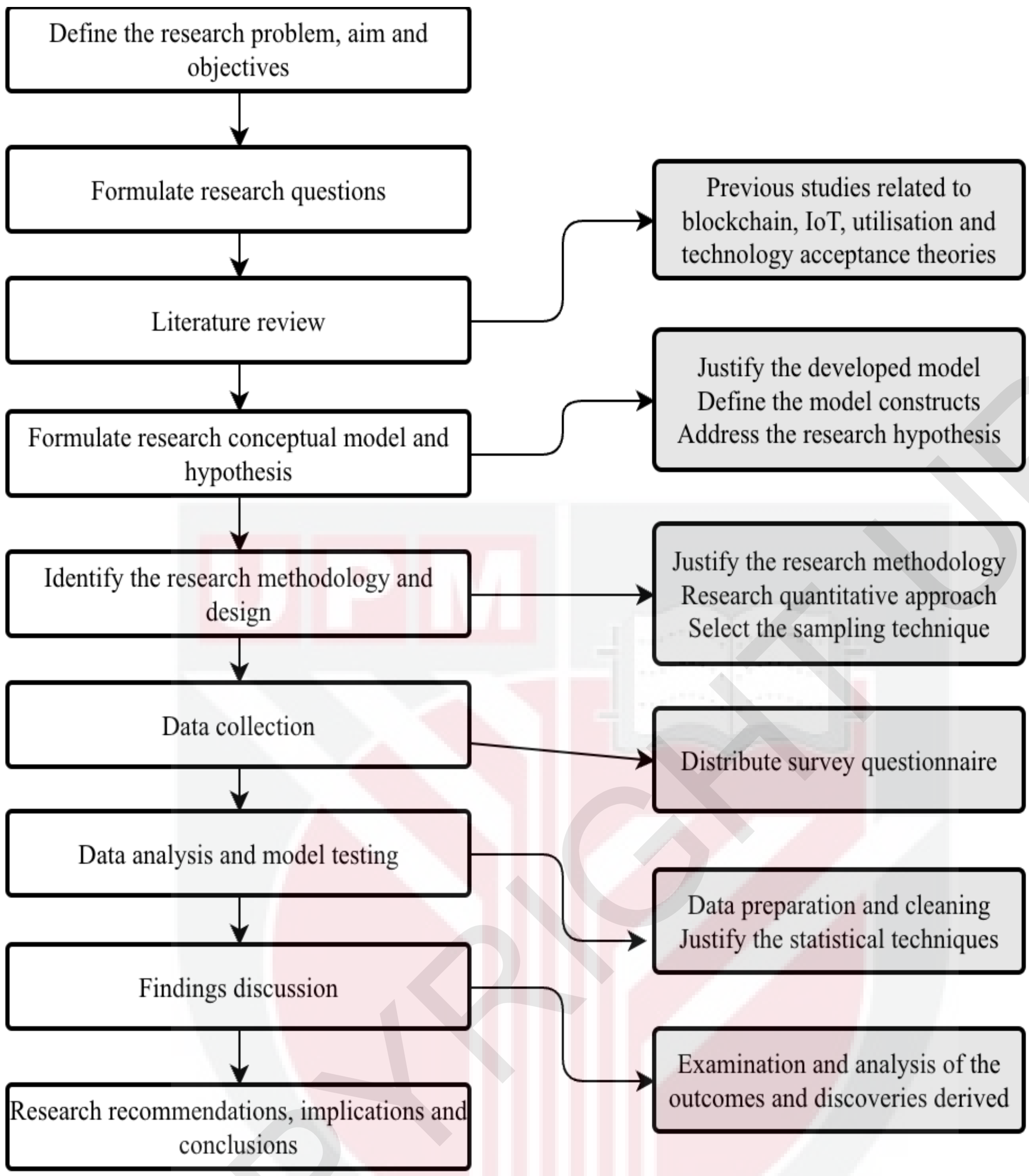

Figure 1.1 : Research Activities

This flow of activities offers a systematic methodology for addressing the research questions and hypotheses, ensuring a comprehensive investigation into the integration of Blockchain technology within the Malaysian IoT ecosystem.

1.9 Chapter Summary

This chapter presents a detailed overview of the research work, situating the study's focus on the integration of Blockchain technology within the IoT ecosystem in

Malaysia. It begins by emphasizing the significance of the research, highlighting the increasing relevance of Blockchain as a solution to critical challenges faced by IoT ecosystem. This is refined to research objectives aimed at assessing the perceived usefulness of Blockchain, evaluating awareness levels among IoT developers, and exploring trends in adoption. These objectives are supported by specific research questions that guide the study, ensuring alignment with the identified problem statement within the current IoT landscape.

Additionally, the research hypotheses are clearly defined, proposing relationships among the perceived usefulness of Blockchain, levels of awareness, and adoption rates within the Malaysian IoT ecosystem. This theoretical grounding establishes a framework for the subsequent methodological approach, which details a quantitative methods strategy for data collection and analysis. The flow of research activities is systematically outlined as well, detailing each phase of the study from literature review to data finding discussion. This structured approach underscores the methodological rigor designed to yield actionable insights and contribute to the expanding body of knowledge in the field.

In summary, this chapter lays a strong foundation for the research by integrating key components that will be examined in subsequent chapters. The emphasis on Blockchain's utility, the significance of awareness, and the trends in adoption are positioned as critical areas for understanding how this technology can enhance the effectiveness of IoT in Malaysia. The findings are anticipated to provide meaningful contributions to both academic and practical applications within the industry.

1.10 Thesis Organisation

Chapter one focuses on the overview of the study, indicates the problem statement as the reason for this study, research objectives, questions, hypothesis, significance, scope, and finally, the summary of the chapter. This chapter further elaborates on the concepts of this study, which entail the researcher focus on developing this research study.

Chapter two on the other hand focuses on the independent variables (blockchain usefulness), (blockchain awareness) and (blockchain adoption) on how it relates towards the dependent variable IoT as the primary purpose of this study. In addition, this chapter also identifies the research theories, models, research gaps, and research hypotheses to analyse the research study effectively.

Chapter Three describes the entire research methodology such as; research approaches, strategy, research technique, method of data collection, research design, questionnaire design, qualitative or quantitative analysis, statistics tools for analysis, pilot study, and procedure to generate the data from the respondents. IBM-SPSS is used for this study analysis.

Next, chapter four focuses on the result generated from the field data and discussion on data entry after examining missing data, field study data analysis, respondents' demographic profile, and description of the study construct. It also describes the processes used to validate the measurement model through regression analyses under which hypotheses are tested. All this is to determine the desired result effectively and also to determine if this study is significant towards its dependent variable or not.

Emphasis is being implemented in this chapter as it helps to provide the researcher with an angle of effective conclusion and recommendation for further studies.

Chapter Five of this thesis presents the discussion on the hypothesis, suggestions for improvements, theoretical & managerial contribution of study and recommendations for further studies. It gives the researcher a comprehensive analysis to conclude the research study effectively. This chapter is considered the summary of the findings, analysis, interpretation and recommendation for further studies. It is essential as it emphasises the comprehensive research study adequately.

CHAPTER 2

LITERATURE REVIEW

This chapter delves into the independent variables blockchain usefulness, blockchain awareness, and blockchain adoption and their relationship with the dependent variable, IoT ecosystem, which forms the central focus of this study. Furthermore, this chapter explores the relevant research theories, providing the study. it also outlines the research hypotheses, offering a structured framework to guide the investigation.

2.1 Systematic Literature Review (SLR)

This section presents a systematic literature review (SLR) conducted to explore the integration of blockchain technology with the Internet of Things (IoT), focusing on its perceived usefulness, awareness, and adoption trends. The SLR follows the guidelines outlined by Kitchenham and Charters (2007) to ensure methodological rigor and transparency. By synthesizing existing literature, this review aims to identify the key challenges, benefits, and research gaps within the context of blockchain-enabled IoT systems, particularly in Malaysia.

2.1.1 Objectives

The primary objectives of this SLR are:

i. To assess the perceived usefulness of Blockchain technology within the IoT ecosystem in Malaysia.

ii. To evaluate the level of awareness and understanding of Blockchain technology among IoT developers in Malaysia.

iii. To assess the adoption rate of Blockchain technology in the Malaysian IoT ecosystem.

2.1.2 Methodology

The SLR was conducted using a structured approach, adhering to the following steps:

2.1.2.1 Research Questions (RQs)

The SLR is guided by the following research questions:

i. How do IoT developers in Malaysia perceive the usefulness of Blockchain technology in addressing key challenges within IoT?

ii. What is the current level of awareness and understanding of Blockchain technology among IoT professionals in Malaysia?

iii. What are the current adoption trends of Blockchain technology within the Malaysian IoT ecosystem?

2.1.2.2 Search Strategy

The following digital libraries were searched for relevant literature:

- SpringerLink
- ScienceDirect
- Google Scholar
- IEEE Xplore
- ACM Digital Library

Search terms included combinations of keywords such as "blockchain," "IoT," "adoption," "awareness," "usefulness," and "integration." Boolean operators (e.g., AND, OR) were used to refine the search queries.

2.1.2.3 Inclusion and Exclusion Criteria

- Inclusion Criteria:

- Peer-reviewed articles published between 2018 and 2024.
- Studies focusing on blockchain and IoT integration.
- Research addressing awareness, adoption, or usefulness of blockchain in IoT.

- Exclusion Criteria:

- Studies addressing non-engineering aspects (ethical or purely commercial issues).
- Duplicates and non-English publications.

2.1.2.4 Study Selection

A total of 75 papers were initially identified. After applying inclusion and exclusion criteria, 30 articles were selected for detailed analysis. The selection process involved two rounds of screening: one based on titles and another on abstracts.

2.1.3 Data Extraction

Key data points were extracted from each study, including:

- Objectives and scope.

- Research methods and findings.
- Contributions to blockchain and IoT integration.

2.1.3.1 Quality Assessment

The quality of the selected studies was evaluated using a checklist based on:

- Relevance to the research questions.
- Methodological rigor.
- Clarity and reliability of findings.

2.2 Background of Study

The IoT and blockchain technology represent two pivotal advancements that have garnered considerable scholarly interest due to their potential to revolutionize diverse sectors (Issa et al., 2023). IoT encompasses the networked interconnection of physical entities—such as devices, vehicles, and infrastructure—that are equipped with sensors, software, and connectivity features (Lao et al., 2020). This interconnectivity enables the collection and exchange of data, which can enhance the operational efficiency and performance across multiple domains, including supply chain, transportation, healthcare, energy, and manufacturing (Ahi and Singh, 2019).

Conversely, blockchain serves as a decentralized digital ledger that facilitates secure and transparent transactions among parties without the necessity for intermediaries (Chaganti et al., 2023). Its architecture is founded upon a network of immutable nodes that validate and securely store information (Chatziamanetoglou and Rants, 2023), rendering it particularly suitable for the management and dissemination of sensitive data.

The unification of IoT and blockchain can yield robust and scalable IoT ecosystems, thereby optimizing data exchange among devices, systems, and stakeholders (Bali et al., 2022). The integration of blockchain offers a secure and tamper-resistant record of IoT-generated data, while IoT contributes real-time insights essential for initiating and executing blockchain transactions (Govindan et al., 2023). This synergy holds particular promise for applications demanding high-security levels, such as financial transactions, supply chain management, and healthcare systems (Khan et al., 2021). Moreover, the unification of these technologies can enhance the efficiency and transparency of various operational frameworks, thereby fostering sustainability and cost-effectiveness (Al Sadawi et al., 2021).

2.3 Blockchain Technology

Blockchain makes available an effective technique to record digital transactions data or interactions, thereby making them safe, transparent, highly anti-interference and verifiable. This technology is still a new technology and is developing rapidly. It will take several years to be in the commercial market. However, key industry decision-makers and significant business sectors that require security and transparency need to immediately focus on blockchain technology and involve their research and development team to study the application of the technology to their business (Stanciu, 2019).

Different authors have different meanings to blockchain technology. In reference (IBM, 2015), it is defined as "a database of distributed records, or a general record of all digital transactions or events that have been executed and shared between participating nodes". With the consent of most nodes participating in the chain network, all transactions made within the record are verified. Once consensus is reached and verified by all nodes, data generated can't be deleted or modified. This is why the blockchain offers a secure and verifiable data record of all transactions in the network.

Although blockchain technology is in the experimental phase, it is seen as a groundbreaking answer to up-to-date technological problems such as data ownership, identity, data-driven decision-making, decentralisation and third-party trust (Zubaydi et al., 2023). The concept of blockchain is that all generated transactions are stored in one block and chained to form a database of different transactions. After creating a new transaction, the sending node transmits a copy of the transaction data to the network for all other nodes through a peer-to-peer communication channel. The transaction is still new and has not yet been confirmed. When a node receives a transaction, it will verify it and store it in its public ledger (Verma & Arora, 2022). The transaction verification is then completed by performing predefined validations on the transaction's data type structure and operation. Different types of nodes called miners in the network are third utilised to generate new blocks, which is then included in some or all of the transactions available at the moment in a transaction pool.

Once this process is completed, the block of the current time-stamp is mined, the mining process holds true for finding a new block title as proof of work. Proof-of-work refers to the search and continuous calculating of the block transaction hashes that match a specified difficulty target. When it comes to mining, more computational capability is required, requiring a specific set of equipment and hardware for the processing. The miner with the correct hash key receives a particular network reward, and the harsh block found joins the continuous blockchains of other blocks in the network. Since the blockchain network records transactions and data based on the new block found, all recent transactions and data are saved to the last block, and this process continues for other blocks and subsequent transactions and data (Stallings, 2015).

In the blockchain network, when a new block is found and generated, it is time-stamped and shared with all the nodes in the network to keep a copy of the new block. When each node receives the node, it is then verified, validated and stored in its ledger. In this process, when all the nodes involved in the network at the current time-stamp accept the generated block, the block becomes a known, unmodifiable and unrecoverable chain of the network. This way, data entered cannot be changed again, and each copy of the block hash value and metadata are stored and are continuous in the next block. This process of each generated block having the hash value and metadata of the previous block (parent block) ensures maximum security in the network.

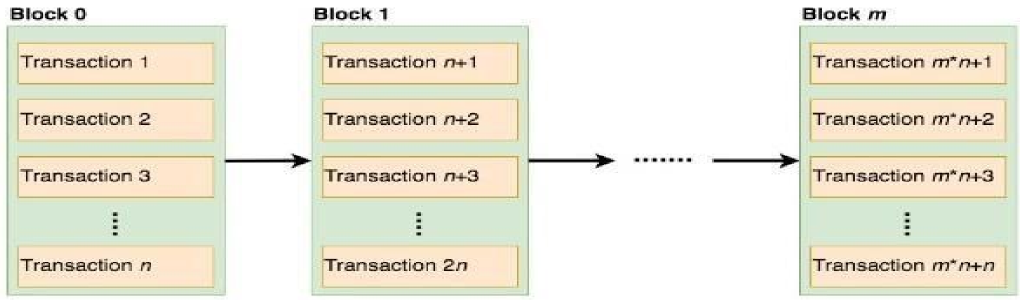

Figure 2.1 : Structure of Blockchain (Xue et al., 2023)

This process explains how the block of each transaction is chained, generated, linked and known as a blockchain, as shown in figure 2.1 above. For data and transaction verification, any person with the right keys known as the address can utilise the address to verify the transaction. This way, the person stays anonymous and can only be identified with the public key. In addition, transactions and data generated within the blockchain are encrypted. Any attempt to attack the network is not possible since the consensus of the other nodes is required to validate each block, except all the nodes online are malicious. Invalid blocks, data and transactions are rejected (Stallings, 2015). The core of blockchain are two main vital things

Transactions: data created by participating nodes.

Chained Blocks: keep a copy of the generated data and ensure that all child blocks have a parent block to prevent data from being tampered with.

2.3.1 Blockchain Characteristics

Blockchain is known to have many characteristics, and these are better suited for IoT current issues and extremely attractive in solving many of its problems. According to (Rejeb et al., 2023), the attributes of blockchain includes:

Anonymity: is an effective way to hide the identity of users and maintain the privacy of their identity, and this feature is significant in today's era of data privacy control.

Immutability: All centralised databases can be ruined or data tempered, and it is necessary to trust a third party to maintain the shared data integrity. Once the user completes any transaction and posts it, it cannot be edited again. This is where blockchain offers an unchanging ledger.

Security: Since all new blocks are dependent on the previous block, blockchain technology offers no point of failure. It provides better security to the entire network where it cannot just be shut down for any or whatever reason.

Decentralisation: Lack of centralised control offers to use the resources of all participating nodes to ensure scalability and flexibility and eliminate many-to-one traffic, thereby reducing delay and solving single point of failure problems, a defect existing in the centralised model.

Capacity: One of the most critical elements of blockchain is its capacity to expand the network's overall size due to participating nodes' options. This means that there are thousands of computers running, which are more powerful than a few centralised servers.

2.4 Internet of Things (IoT) Overview

Generally, the IoT is a group of tiny computer devices, servers, physical nodes and small objects integrated into a network system (Ongaro et al., 2007). The well-known areas of IoT applications are smart homes (Merke, 2014) and intelligent cities (Atzori et al., 2010), intelligent vehicle systems (Kaur et al., 2023) and intelligent health care networks systems (Zanella et al., 2014), where they are widely distributed. With the emergence of advanced computing technologies, the development of traditional cloud centralised architectures has been fast-tracked (Queralta et al., 2019; Mutlag et al., 2019). The purpose of the unified standard classification is to ensure that the structure of the IoT is consistent and that it continues to develop. The service, platform, network, and node (device) layers are all covered by this framework (Qingqing et al., 2019). A comprehensive review of security attacks on wireless sensor networks (WSNs) and the IoT is included in reference (Shi et al., 2019), as well as strategies to avoid, detect, and mitigate these attacks. Many networked IoT devices that create enormous amounts of data make up an IoT network. At the same time, IoT devices typically have limited processor and memory capabilities and performance and battery life. As a result, it can be described as a limited-capability device that can withstand various hacker cyber-attacks. This chasm leads to concerns about security and privacy. New technologies have emerged to meet these issues of IoT centralization, among which blockchain is one of the most promising.

2.5 IoT and Blockchain

Many IoT applications are susceptible to problems like system failures and data leaks (Lee et al., 2019). This is where blockchain technology might help solve these problems by providing improved security and scalability for IoT applications. Nevertheless, the tasks related to real-time executing current methods are numerous. They involve the division of labour between IoT devices and the limited functions of IoT devices, such as processing power and memory capability, performance, and battery level resources. Many research papers on blockchain technology are dedicated to solving the challenges of using blockchain in the IoT (Lee et al., 2019; Butun et al., 2019; Bahga et al., 2019). Some vendors of decentralised and distributed IoT systems have employed and implemented blockchain technology in their services to ensure trust (Liu et al., 2023), data protection and security (Rahman et al., 2023), data management and accessing (Arshad et al., 2023), fault detection and tolerance (Falayi et al., 2023), and peer-to-peer transactions (Xie et al., 2023). The nature of blockchain platforms depends on how the user handles credentials and are divided into three main types: (i) public or permissionless blockchains, (ii) private or permission blockchains, and (iii) consortium blockchain. Blockchains that can be merged by anonymous nodes (devices), read data and participate in data exchange in equal states are known as the public blockchain. In contrast, private blockchains or consortia are based on permissions granted to various nodes and must be authenticated to perform specific operations (Su et al., 2014).

When it comes to blockchain use with IoT, scalability is the main issue. Several research articles have solved the scalability problem in the Bitcoin architecture (Vemula, 2023), where Bitcoin is an application that employs blockchain technology for FinTech solutions. Smart contracts are a promising technology that can allow IoT and blockchain to be integrated. But its performance and scalability are in a straight line related to the overall performance of the blockchain system (Naaz et al., 2023). Some IoT applications and vendors have recently used blockchain for smart contract services, digital payments (Karame, 2016), and data storage and management (Ucbas et al., 2023). However, continuing advancements in new technologies can help next-generation blockchain systems achieve greater scalability and performance. A layer-based IoT blockchain framework has been proposed in several works and literature to address the difficulty of extending IoT systems while improving performance and security. Through the integration of smart devices and blockchain technology, the layer-based structure is predicted to provide a security solution for smart cities (Christidis, 2016). In multi-layer platforms, hybrid network architecture can leverage blockchain technology and software-defined networking (SDN).

In contrast, layer-based blockchain can solve IoT system issues, including resource usage and reaction time (Peng et al., 2019). (Biswas et al., 2016). This technique can further facilitate the integration of blockchain technology into IoT systems by overcoming the difficulties of implementing blockchain in a layer-based paradigm (Shankar & Maple, 2023). In reference (Mbarek et al., 2019), the security problems associated with smart city cyber-physical systems (CPS) have been discussed, and recommendations for the use of anomaly detection systems distributed by smart city CPS have been proposed. To safeguard encrypted photos, a paper by Xuan et al. (2019) presented a blockchain-based solution based on private authorization in the context of the Industrial IoT. While Butun & Österberg, (2019) introduce the latest conditions of industrial automation to better understand possible technologies, profit potential, and challenges of Industry 4.0 and IIoT, this method stores the encrypted pixel value of the image on the blockchain to ensure the privacy and security of the image data. In contrast, Butun et al. (2019) introduce the latest industrial automation conditions to understand better possible technologies, profit potential, and challenges of Industry 4.0 and IIoT. It also addresses the security needs of users and IIoT services in terms of network security.

2.5.1 Blockchain for Edge Computing

Several researches have been done on merging of blockchain technology and advanced edge computing layers in recent years. Many articles focus on establishing safe and effective advanced distributed computing (Butun et al., (2019); Khan et al., 2019). The integration is designed to improve security and adopt blockchain technology to create access management and control strategies for various edge applications (Butun, 2020; Apat et al., 2023; Queralta et al., 2020; Dai et al., 2019). In reference (Yadav & Sharma, 2023; Alzubi et al., 2023), both authors focused on resource management through blockchain. The automation of distributed robotic systems is also being considered (Samaniego et al., 2016). Blockchain integration with edge computing also provides substantial advantages in advanced computer security (Chatziamanetoglou et al., 2023). Combining blockchain permissions and distributed ledger technology (DLT) with distinctiveness management can solve many challenges by increasing layer flexibility while ensuring network traffic integrity to prevent tampering and dangerous traversal manipulation. Through blockchain-based resource management, fraud in manipulating network resources and the use of shared resources can be avoided. In addition, blockchain technology has been adopted in the automotive industry (Queralta et al., 2020) and in the health field (Soldani et al., 2019) to deliver a higher level of security. Blockchain is, in some cases, used to bring a decentralised authentication model for the IoT and edge computing situation (Kureshi et al., 2023). The blockchain applications and acceptance processes are further explored to improve confidentiality, integrity, and permitted authentication control between clouds in IoT, edge computing, and connected 5G and IoT telemedicine systems (Ma et al., 2020). Hewa et al. (2020) proposed an HLF-based blockchain architecture in the health care sector to monitor and notify patient data and health. In reference to (Attia et al., 2019), the authors emphasised the significance and advantages of fog computing in IoT networks. They conducted an in-depth study on the physical safety of fog devices through a rich, in-depth literature review. In reference (Butun et al., 2020), a blockchain-based HLF model is introduced as a service to meet the specific needs of IoT systems, including very low storage, hardware, and network connectivity capacity.

2.5.2 Blockchain for Data Sharing and Traceability

Message Authentication Codes (MAC) and Digital Signatures (DS) are the two recognized approaches for detecting data's origin and heredity. Yet, these cryptanalytic procedures cannot make available complete data proof (Peši´c et al., 2019). In addition, using data from different nodes to manage keys in a heterogeneous IoT network is also complex. Even though log-based solutions can help with data transfer and system event monitoring, they can't correctly track data in remote IoT systems (Heller et al., 2012). Blockchain technology has long been considered a data source for distributed systems like the IoT. Data operation is included in blockchain transactions to provide data sources (Suen et al., 2013). ProvChain by Yeboah-Ofori et al. (2023) is a decentralised blockchain-based data source architecture that can enable data verification and integrity in a cloud context. The blockchain network keeps track of data operations (Mahalakshmi et al., 2023), such as data sources in blockchain transactions, and maintains the records in a local ledger. Without the need for off-chain authentication, smart contracts can automatically run complex blockchain-enabled systems (Celik et al., 2023). The data transmission tracking function is provided in the smart contract with built-in access rules to protect the confidentiality of the data in the distributed ledger (Dolhopolov et al., 2023). SmartProvenance

(Narayan et al., 2023) is a distributed proof of blockchain-based data system. It simplifies the verification of original records and uses smart contracts and open-source models (OPM) to provide reliable data collection and evidence. The blockchain has been presented to verify that industrial activities are safe and trustworthy (Latif et al., 2020). Because of the complexity of blockchain implementation, the above-mentioned original technologies cannot be implemented in IoT systems. Existing data source research is complex and expensive from a computational standpoint. As a result, this strategy is not practicable for resource-constrained IoT systems with restricted processor performance, memory space, and battery capacity.

Although blockchain has advantages in IoT applications, resources related to integration are limited, and scalability also faces challenges (Atlam et al., 2018; Xue et al., 2023). In general, the blockchain demands high computing power, low latency, and high bandwidth for the Proof of Work (PoW) mining process. Blockchain mining is not possible on IoT devices with minimal computing capacity. In most cases, data encryption takes place in the blockchain system. The entire blockchain process uses very little energy, which is ideal for IoT devices. The storage capacity of most IoT devices is relatively modest, but the size of blockchain devices continues to grow. Because it necessitates a vast memory capacity, storing a replica of a complete blockchain device for IoT devices is not practical. The blockchain storage capacity for Bitcoin surpasses 200 GB, whereas Ethereum's storage capacity is over 1.5 TB. Nodes must share regular information through a consensus process in the new generation of blocks and blockchain agreements. High bandwidth and low latency are required for the consensus process and information exchange. IoT devices, on the other hand, frequently have restricted bandwidth. The necessity for high scalability in blockchain networks is a common source of worry for blockchain systems (Buterin, 2014). The risk of centralization is a worry with massive blockchains. A vast number of networked devices are present in many IoT systems. In addition, by adding or removing IoT devices, IoT networks are frequently adjusted to adapt to different applications (Jahid et al., 2023). As a result, solutions are required to address the problem of increasing IoT systems. Furthermore, IoT device processing power and storage capacity restrictions on the blockchain network must be addressed.

2.6 Related Studies on Blockchain

The related works depicted in this section primarily focus on adoption intentions, awareness, usefulness, and legislative concerns related to blockchain. Given that blockchain represents an emerging technological innovation, it is unsurprising that much of the scholarly attention has centered on understanding the behavioral intentions driving the adoption of blockchain, especially in the context of cryptocurrencies such as Bitcoin. Several studies have specifically examined the factors influencing adoption intentions for cryptocurrencies and Bitcoin, including works by Chen et al. (2022), Yeong et al. (2021, 2022), Sukumaran et al. (2022), and Miraz et al. (2022), as well as Angeline et al. (2021).

A significant body of research has also focused on the level of awareness of blockchain within specific communities, with a particular focus on Malaysia. For example, Ku-Mahamud et al. (2019) assessed the awareness of blockchain technology among the Malaysian blockchain community. Meanwhile, Muhamad et al. (2020) explored the acceptance of data-sharing practices within Malaysia's intelligence community, with an emphasis on blockchain 's role in such activities. Furthermore, some studies have examined the pivotal role of trust in the adoption and usage of blockchain. For instance, Miraz et al. (2020) investigated the trust-related challenges in utilizing blockchain and Bitcoin for peer-to-peer money transfers, while Sas and Khairuddin (2017) addressed user experience and trust issues associated with Bitcoin. Additionally, Miraz et al. (2020a) explored how trust mediates the factors influencing the adoption of blockchain in e-logistics.

Another important area of blockchain has been the development of appropriate legislative frameworks to support the adoption of blockchain. Baskaran et al. (2020) examined the intersection between blockchain and Malaysia's Personal Data Protection Act 2010 (PDPA), identifying critical regulatory components that may conflict with the implementation of blockchain in the country. Similarly, Zain et al. (2019) analyzed the legal challenges faced by Malaysia in implementing blockchain-based smart tenancy systems, focusing on the current state of smart contracts in Malaysia and the adequacy of the national legal framework to accommodate recent technological developments.

In terms of the conceptual and economic implications of blockchain, existing research delves into its potential, roles, and the industrial and economic impacts it may have across various sectors. Notably, Hira et al. (2022) examined how blockchain could address ongoing issues in Malaysia's healthcare industry. Other studies have focused on the application of blockchain in Malaysia's construction industry (Kiu et al., 2024; Bolhassan et al., 2022), as well as its use for managing waqf (Islamic endowments) (Abd Razak et al., 2020).

Several studies have also investigated the role of blockchain in supply chain management. Tan et al. (2023) explored the correlations between blockchain visibility, supply chain integration, and supply chain performance in Malaysia's semiconductor sector in the context of digital transformation. Khan et al. (2022) analyzed the direct impact of blockchain on the sustainability of supply chains in electrical and electronics firms. Mubarik et al. (2021) examined how blockchain influences green supply chain practices and promotes environmentally sustainable practices within manufacturing enterprises. Additionally, the role of blockchain in facilitating supply chain integration has been highlighted (Mubarik & Mubarak, 2020), along with its significance in fostering circular economy activities and enhancing organizational performance (Khan et al., 2021, 2022).

Further contributions to the body of literature include Miraz et al. (2019), who examined the impact of blockchain and Bitcoin on Malaysian marketplaces, and Yavuz et al. (2020), who assessed whether blockchain could resolve trust issues within the Islamic interbank monetary system. These studies collectively contribute to the growing body of knowledge regarding the multifaceted implications of blockchain across different industries and sectors.

2.6.1 Blockchain Implementation Challenges from Past Studies

The integration of blockchain technology and the IoT holds the potential to significantly transform various sectors; however, this convergence also presents several limitations and challenges. The integration of blockchain with IoT, often referred to as Blockchain-enabled IoT (BIoT), is subject to a range of technical and operational constraints that hinder its widespread implementation. This section aims to elucidate the primary obstacles associated with BIoT integration and outlines the key areas that require further resolution.

The IoT devices are predominantly powered by batteries, making energy efficiency a critical concern in the design of Blockchain-enabled IoT (BIoT) architectures. In contrast, blockchain technologies, by nature, tend to consume significant amounts of energy, posing a substantial challenge when integrated with IoT systems. Two primary factors contribute to the high energy consumption of blockchain systems: (1) the consensus algorithms, such as Proof of Work (PoW), which require vast amounts of electrical power for the process of mining, and (2) the necessity for edge devices to remain active during peer-to-peer (P2P) communication, which leads to excessive energy consumption (Fraga-Lamas et al., 2024; Safavi et al., 2022).

To mitigate these energy-related issues, several energy-efficient P2P protocols have been proposed in recent literature (Wu et al., 2022; Bada et al., 2021; Boumaiza, 2024). In terms of optimizing consensus algorithms, Ball et al. (2021) suggested that the energy expended in PoW could be redirected toward more productive activities. Additionally, alternative consensus mechanisms, such as Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT), have been proposed as solutions to reduce energy consumption in blockchain networks (Stathakopoulou et al., 2022).

With regard to P2P communication, each blockchain update requires considerable energy to process new blocks. A potential solution to this issue involves the use of mini-blockchains, which allow for more direct interactions between IoT nodes and the blockchain, bypassing the need for extensive updates across the entire chain (Gordon, 2020). Furthermore, the development of fast-hashing algorithms, such as Spongent (Apriani & Sari, 2021), Photon (Hatanaka et al., 2024), and Blake-256 (Özcan et al., 2022), has been proposed as a means of reducing power consumption associated with blockchain operations. These advancements collectively aim to strike a balance between the energy demands of blockchain and the power limitations of IoT devices.

Additionally, IoT devices face significant constraints in terms of storage capacity, despite their ability to generate gigabytes of data in real-time. This limitation poses a considerable challenge when attempting to integrate blockchain with IoT devices in real-time applications. Current blockchain technologies, such as Bitcoin, are designed to process a limited number of transactions per second, which exacerbates the difficulty of applying blockchain to IoT environments, where large volumes of data need to be processed rapidly and efficiently. Blockchain, in its current form, is not optimized for storing vast amounts of data, making it unsuitable for the real-time demands of IoT systems. However, several techniques for data compression, normalization, and filtration have been proposed in the literature to address the storage challenges in IoT applications (Na & Park, 2021; Wang et al., 2022; Yu et al., 2020). These approaches help lighten the burden of data transmission and storage within blockchain networks, facilitating more efficient integration of IoT data with blockchain.

Blockchain inherently requires data storage to maintain the authenticity and integrity of the information it handles. Once data is added to a blockchain, it cannot be deleted; rather, new transactions are appended to the ledger, maintaining a permanent record. The process of reading the blockchain often involves downloading the entire ledger, which can take several days (up to four days to download the complete Bitcoin ledger). Given the limited storage capabilities of IoT devices, this mechanism is impractical for real-time IoT applications. Several potential solutions have been proposed, such as sharing the storage of the Unspent Transaction Output (UTXO) data structure, but these solutions remain unclear in terms of their scalability and their interaction with other types of blockchain data, such as smart contracts (Chakravarty et al., 2020; Bartoletti et al., 2024).

A notable alternative to address the challenges posed by large volumes of data and high transaction throughput in IoT environments is Tangle, a distributed ledger technology introduced by Popov for the IOTA cryptocurrency (Kraner et al., 2023). Tangle, which is based on a Directed Acyclic Graph (DAG) rather than a traditional block-and-chain structure, aims to resolve blockchain's issues with transaction fees and scalability. In Tangle, transactions are confirmed by a group of peers, reducing transaction fees and increasing transaction throughput (Khan et al., 2024). Additionally, Tangle offers enhanced scalability by creating smaller data structures that do not require the inclusion of complete transactions in each update (Abdullah et al., 2023). By discarding the conventional blockchain architecture, Tangle presents a promising solution to the scalability and fee challenges typically faced by blockchain systems. However, the primary drawback of this approach is the potential for centralization, which could compromise the decentralization principle that underpins blockchain's security and trust mechanisms.

The unregulated nature of blockchain technology has played a crucial role in the success of cryptocurrencies, particularly in enabling decentralized financial systems.

However, for virtual currencies, one of the major controversies revolves around their legal status and regulatory frameworks (Makhija, 2024). In response to these concerns, there has been a growing interest in introducing more controlled networks through the use of private, permissioned, and consortium blockchains. These frameworks allow for greater oversight and regulatory compliance while maintaining some of the core principles of blockchain technology. With the rise of IoT, the implementation of blockchain faces additional challenges, particularly related to data privacy and compliance with legal requirements. In the IoT ecosystem, regulations such as the General Data Protection Regulation (GDPR) in the European Union, as well as other directives focused on data protection, have been increasingly adopted (Antoniewska, 2023). However, the application of these privacy laws in conjunction with blockchain technology presents significant hurdles. Blockchain's inherent immutability and transparency can conflict with privacy regulations that require data to be mutable or deleted upon request, creating a tension between blockchain's decentralized model and the centralized control often needed for compliance with data privacy laws.

In some IoT applications, there is a vision for a globally unified blockchain to manage data across devices, but the governance and management of such a system remain unclear (Adeghe et al., 2024). This lack of clarity raises questions about the adoption of the blockchain network, how decisions would be made, and how users or managers would be authorized to control data. These uncertainties imply that, in many cases, legal authorization and formal regulatory approval would be required for the deployment of such systems. As a result, the integration of blockchain with IoT is increasingly constrained by these legal and regulatory frameworks, which challenge the decentralized ethos that blockchain was initially designed to uphold. The introduction of private or permissioned blockchains, which impose centralized control over the participants, risks undermining blockchain's core principles of openness and decentralization (Mustafa et al., 2024).

2.6.2 Research Impact and the Formulation of Proposed Objectives

The objectives of this thesis are rooted in the identification of key challenges and gaps that hinder the integration of Blockchain technology into Malaysia's IoT landscape. These challenges primarily revolve around three interconnected factors: perceived usefulness, awareness, and adoption trends. Together, these factors present significant barriers to the effective deployment of Blockchain within this context. The following outlines the critical impacts that have shaped the research objectives:

Perceived Usefulness

Impact: Although Blockchain holds significant promise for improving security, transparency, and efficiency within IoT applications, many stakeholders in Malaysia remain uncertain about its tangible benefits. Concerns about its energy consumption, scalability issues, and high implementation costs often overshadow its potential advantages.

Relevance: Gaining a deeper understanding of how Malaysian IoT developers and businesses perceive Blockchain's value is crucial. This insight can help identify key factors that influence its adoption and highlight areas where further education or technological improvements are necessary.

Objective 1: To assess the perceived usefulness of Blockchain technology within the IoT ecosystem in Malaysia.

Awareness and Understanding

Impact: A notable gap exists in the awareness of Blockchain's capabilities and limitations among IoT developers in Malaysia, which contributes to its slow adoption. Many developers lack a comprehensive understanding of how Blockchain can be applied effectively in IoT environments.

Relevance: Assessing the current level of awareness will help identify knowledge gaps, enabling targeted educational initiatives to increase understanding and encourage wider acceptance of Blockchain among IoT professionals in Malaysia.

Objective 2: To evaluate the level of awareness and understanding of Blockchain technology among IoT developers in Malaysia.

Adoption Trends

Impact: Blockchain adoption within Malaysia's IoT sector has been sluggish, hindered by challenges such as regulatory uncertainty, concerns over energy inefficiency, and limitations in data storage capabilities. The absence of clear adoption trends or successful case studies further discourages organizations from considering Blockchain solutions.

Relevance: Understanding current adoption rates is essential to identify the barriers impeding Blockchain's integration into Malaysia's IoT ecosystem. This will help inform strategies for overcoming these challenges and accelerating its adoption.

Objective 3: To assess the adoption rate of Blockchain technology in the Malaysian IoT ecosystem.

2.7 Research Gap

The research gap in this study lies in the limited exploration of the integration of Blockchain technology within the Internet of Things (IoT) ecosystem in Malaysia, particularly from the perspectives of IoT professionals. While there is extensive literature on the individual impacts of Blockchain and IoT, few studies have comprehensively addressed how the adoption and perceived usefulness of Blockchain can shape the future of IoT infrastructure in emerging markets like Malaysia. While Blockchain adoption has been studied in global contexts, there is a lack of in-depth research focusing specifically on Malaysia's IoT ecosystem. This study addresses this gap by exploring how Blockchain is perceived and its potential role in enhancing IoT applications within Malaysia.

Much research has been conducted on Blockchain awareness in developed countries, the level of awareness and adoption of Blockchain in IoT among developers in emerging markets like Malaysia is underexplored. The study addresses this gap by assessing the awareness and adoption levels of Blockchain technology among Malaysian IoT professionals. Furthermore, models like the Technology Acceptance Model (TAM) have been widely used to assess technology adoption, their application in the specific context of Blockchain within the IoT sector is limited. This study uses TAM to explore how perceived usefulness, awareness, and adoptability influence Blockchain adoption in Malaysia's IoT ecosystem. By addressing these gaps, this study contributes new insights into how Blockchain can be successfully integrated into the IoT ecosystem, particularly in Malaysia, and provides a foundation for future research in similar emerging markets.

2.8 Theoretical Framework

The primary goal of the Technology Acceptance Model (TAM) was to elucidate the processes that underlie technology adoption, aiming to predict user behavior and offer a theoretical framework for understanding the successful implementation of technological systems. From a practical standpoint, TAM sought to provide guidance for practitioners, offering insights into the actions they could take prior to implementing systems to facilitate acceptance and ensure success. To achieve these objectives, several methodological steps were undertaken in the development of the model (Davis, 1989).

Davis initiated the creation of TAM by conceptualizing the mediating processes that link Information Systems (IS) characteristics—referred to as external factors—with the actual use of the system. The model was grounded in the Theory of Reasoned Action (TRA), which provided a psychological perspective on human behavior that was notably absent in the Information Systems literature at the time (Davis, 1993). By integrating the TRA framework, TAM offered a more comprehensive understanding of how user perceptions of system attributes, such as perceived ease of use and perceived usefulness, influence technology adoption decisions and subsequent system utilization.

The second step in the development of the Technology Acceptance Model (TAM) involved identifying and defining key variables that would have a strong correlation with system usage, followed by the validation of measures for these variables. Drawing upon previous empirical research on human behavior and Information Systems (IS) management, multi-item scales for the constructs of perceived ease of use and perceived usefulness were developed, pre-tested, and validated through several studies. It was hypothesized that these two constructs were fundamental determinants of user acceptance, supported by prior research (Johnson & Payne, 1985; Robey, 1979). This body of work suggested that an individual's decision to engage in a particular behavior is largely driven by a cost-benefit analysis, where the perceived benefits of performing the behavior are weighed against the effort or costs required to perform it (Payne, 1982). In the context of IS, this implies that system use is determined by the perceived trade-off between the system's usefulness and the effort required to use it (Davis, 1989).

Perceived usefulness was defined as the degree to which a person believes that using a particular system would enhance their performance. This construct drew upon Bandura's concept of outcome judgment, which posits that behavior is influenced by an individual's expectation of positive outcomes (Bandura, 1982). The operationalization of perceived usefulness was grounded in empirical evidence demonstrating the relationship between performance expectancy and system usage (Robey, 1979). On the other hand, perceived ease of use was conceptualized as the extent to which a person believes that using a specific system would be free from effort (Davis, 1989). This construct was inspired by Bandura's self-efficacy theory, which refers to an individual's belief in their ability to perform tasks required for achieving specific outcomes (Bandura, 1982). Self-efficacy was shown to play a key role in decision-making regarding technology use (Hill, Smith, & Mann, 1987). Moreover, perceived ease of use shared similarities with the complexity construct from the innovation diffusion literature, which suggests that the perceived difficulty of understanding and using an innovation can act as a barrier to its adoption (Mahajan, 2010).

The validity and reliability of these constructs were assessed by examining the relationship between self-reported IS usage and the two proposed factors in an organizational setting. The scales developed for perceived ease of use and perceived usefulness demonstrated strong psychometric properties. Further validation of the model was achieved by confirming significant relationships between perceived usefulness, perceived ease of use, behavioral intention, and actual usage behavior (Davis, 1989). These findings provided strong empirical support for the core tenets of the TAM, establishing it as a robust model for predicting and explaining technology acceptance.

According to the Technology Acceptance Model (TAM), technology acceptance is a three-stage process, wherein external factors—such as system design features—trigger cognitive responses (specifically perceived ease of use and perceived usefulness). These cognitive responses then generate an affective response, which is reflected in attitudes toward using the technology or behavioral intention, ultimately influencing actual use behavior (Davis, 1993). TAM conceptualizes user behavior as the outcome of these variables, with perceived ease of use, perceived usefulness, and behavioral intention acting as key predictors (Figure 2.2). Perceived ease of use and perceived usefulness represent the user's expectations of positive behavioral outcomes and the belief that the behavior will not require excessive effort (Davis, 1989).

In subsequent research, Davis (1993) suggested that behavioral intention could be replaced by the attitude toward behavior, which is defined as an affective evaluation of the potential consequences of engaging in a particular behavior (Ajzen, 2011). This shift highlights the emotional or evaluative aspect of technology adoption, where the strength of the affective response directly correlates with the likelihood of engaging in the behavior. In other words, the more favorable the user's attitude toward using the technology, the greater the likelihood of its actual use.

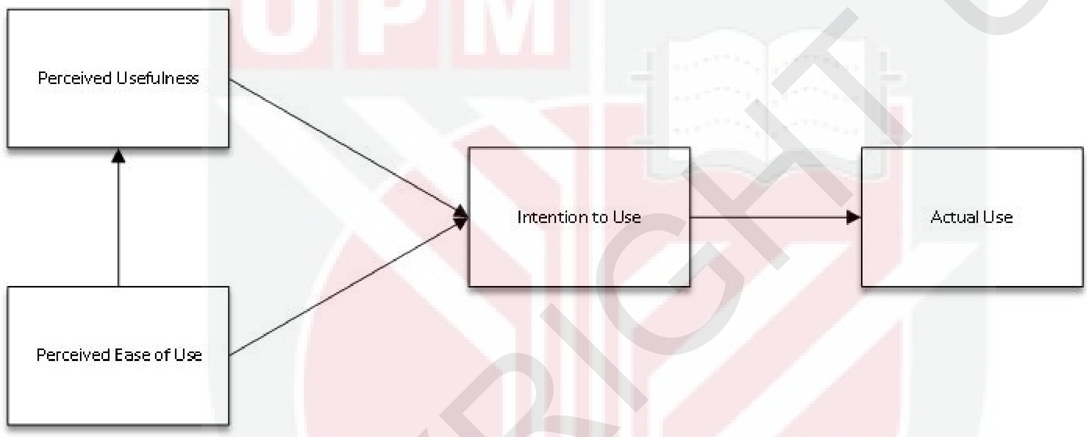

Figure 2.2 : Technology Acceptance Model

Furthermore, the model posits that perceived usefulness can directly influence actual usage behavior, making it a critical predictor of technology adoption. Although perceived ease of use does not directly affect usage behavior, it plays an indirect role by reinforcing the effect of perceived usefulness (Davis, 1993). This suggests that if users perceive an application as easy to use, they are more likely to consider it useful, which in turn increases the likelihood of technology acceptance (Davis, 1989; Davis, 1993). Thus, TAM underscores the importance of both ease of use and perceived usefulness in driving the successful adoption of technology, where ease of use serves as a foundational factor that supports the perception of usefulness.

The development of the Technology Acceptance Model (TAM) and its associated measures has made substantial theoretical contributions to the field of Information Systems (IS) and provided significant practical value. One of the key contributions of TAM is its ability to evaluate the motivation of users to adopt a wide range of technologies. Prior to the development of this model, such evaluations were difficult to conduct due to the lack of validated subjective measures for understanding user acceptance (Hwang, 2005; Gefen, Karahanna & Straub, 2003; Araújo & Casais, 2020). By introducing constructs like perceived ease of use and perceived usefulness, TAM provided a structured framework for capturing the cognitive and affective responses that mediate the relationship between system characteristics and technology acceptance.

These constructs, with their strong and significant correlation to actual usage behavior, allowed for a deeper understanding of the psychological factors influencing technology adoption. Specifically, TAM illuminated the cognitive factors (such as perceived ease of use and usefulness) and affective factors (such as attitudes toward technology) that shape users' decisions to adopt or reject a technology (Davis, 1989). By bridging these internal psychological processes with observable behavior, the model not only advanced theoretical understanding but also enhanced practical applications, enabling more accurate predictions of technology acceptance and informing the design and implementation of user-friendly IS solutions.

2.8.1 Relation to This Research

The integration of Blockchain and the IoT presents unique challenges and opportunities, particularly when viewed through the Technology Acceptance Model

(TAM). The theoretical contributions of TAM, particularly in understanding the factors that drive technology acceptance, can be applied to the adoption of Blockchain in IoT environments.

Blockchain, as a disruptive technology, faces barriers to widespread adoption in IoT applications, especially given its complexity, scalability concerns, and energy inefficiencies. However, applying the constructs of TAM—perceived ease of use and perceived usefulness—can help identify the factors that influence user acceptance of Blockchain-based IoT systems.

Perceived Usefulness: For IoT systems, the perceived usefulness of Blockchain is tied to the promise of enhanced security, transparency, and data integrity. If users or organizations view Blockchain as a technology that can improve the efficiency and security of their IoT applications, this could significantly enhance adoption. For instance, Blockchain could offer decentralized control, secure data sharing, and transparent records of transactions or sensor data in IoT networks. The more users perceive that integrating Blockchain into IoT devices will lead to tangible benefits—such as reduced fraud, tamper-proof data, and enhanced trust—the more likely they are to accept and adopt these systems.

Perceived Ease of Use: Blockchain's complexity, particularly in terms of understanding consensus mechanisms, cryptographic processes, and system management, can pose a barrier to its adoption in IoT environments. If IoT users perceive Blockchain as difficult to implement or manage, it may hinder acceptance. Therefore, Blockchain solutions designed for IoT should focus on making the awareness of these technical aspects and improving user interfaces to increase the perceived ease of use. Simplified consensus algorithms, more efficient integration methods, and better interoperability with existing IoT platforms could make Blockchain more appealing and aware to users.

Cognitive and Affective Responses: Blockchain's adoption in IoT also depends on how users evaluate the technology, both cognitively (rational assessment of benefits like enhanced security and decentralization) and affectively (emotional responses to the idea of trusting a decentralized system). Blockchain's ability to address privacy concerns in IoT, for example, could create a positive affective response, driving higher adoption rates. On the other hand, concerns over the complexity, energy consumption, and regulatory challenges could generate negative responses, limiting acceptance.

The integration of Blockchain and IoT can be better understood through the TAM framework, which helps clarify the cognitive (usefulness, ease of use) and affective (attitude, intention) factors that shape the adoption of new technologies. By focusing on enhancing the perceived usefulness and ease of use of Blockchain within IoT applications, and addressing concerns around complexity and energy efficiency, developers and practitioners can improve the likelihood of successful adoption of Blockchain-enabled IoT solutions.

2.8.2 Key Selection

In this study, key awareness is selected based on the relevance of Blockchain technology to the IoT ecosystem and the factors influencing its adoption. Awareness is a crucial factor in understanding the potential for integrating Blockchain into IoT, as it directly affects the readiness of professionals and organizations to embrace new technologies. The selection of key awareness variables is informed by existing literature and theoretical frameworks, such as the Technology Acceptance Model (TAM), which emphasizes the role of user perception in technology adoption. To select key awareness factors, the study focused on the following:

Perceived Usefulness: This refers to the extent to which IoT professionals believe that Blockchain technology can enhance the efficiency, security, and scalability of IoT systems. As perceived usefulness directly impacts the decision to adopt a technology, it is prioritized in this study.

Knowledge of Blockchain: The study assessed the level of understanding among IoT professionals regarding Blockchain's core functionalities, such as decentralization, smart contracts, and enhanced security. This was considered crucial in determining how well the technology is understood within the IoT context.

Perceived Barriers: Awareness of potential obstacles, such as regulatory issues, technical challenges, and integration complexities, is also evaluated. This provided insight into whether IoT professionals recognize any limitations or concerns regarding Blockchain adoption.

By focusing on these key aspects, the study ensured that awareness was not only about familiarity with Blockchain but also about its perceived value and challenges within the IoT ecosystem. This approach will help capture the readiness and willingness of IoT developers and professionals to integrate Blockchain into their operations.

2.9 Research Hypothesis Development

This section examines the correlation between usefulness of Blockchain, awareness of Blockchain, and adoptability rate of Blockchain with IoT ecosystem practices.

2.9.1 Usefulness of Blockchain with IoT Ecosystem

The benefits of Blockchain technology closely align with the first research objective: to evaluate the perceived usefulness of Blockchain within Malaysia's IoT ecosystem. Blockchain's key attributes, such as its decentralized nature and public accessibility, effectively overcome several challenges associated with traditional, centralized IoT systems. These challenges include high operational costs, limited scalability, and inefficiencies in data transfer. By enabling secure and private data sharing among IoT devices, Blockchain enhances the overall functionality of Malaysia’s IoT infrastructure. Based on the characteristic of the blockchain highlighted above, the combination of blockchain and IoT has many advantages, and these advantages can be summarised as follows:

Public Usage: In blockchain technology, each node in the network can see all transactions and data. However, the data content is only protected with the user (address) key (Samaniego et al., 2016a). Since IoT nodes exchange data with each other, blockchain technology can help allow each node to share data and protect the content with a key and protect user privacy.

Decentralisation: This functionality benefits IoT nodes by enabling distributed data sharing. Instead, all nodes in the network must approve a block, check data, and record it in their ledger. As a result, this feature eliminates the requirement for centralised traffic management in today's IoT architecture.

Sustainability: Each node connected to the network has a copy of the general distributed data in their ledger; this copy of the data holds all the data performed in the network and therefore contains a firm ground against attack to the network. If a single node is compromised, the remaining nodes in the network will manage the network and keep it running (Xue et al., 2023). This feature helps the IoT network form better security and increases the information exchange within the IoT network.

Security: Blockchain offers strong network security based on chain technology; even parties who don’t know themselves can transact and share data. This novel security is essential to the heterogeneous and several nodes of IoT (Kiran et al., 2024). This means that all the IoT nodes connected to the same network need to be attackers to attack the network and successfully tamper with data.

Speed: When it comes to data exchange within a network, Blockchain technology offers speed of data interchange within a few seconds and stays active any time and day (Christidis et al., 2019).

Cost Saving: The current centralised architecture of IoT holds for large server farms, power and processing resources, network equipment and other. These supplies make centralised IoT expensive and more when billions of nodes are connected. The decentralised feature of blockchain mitigates this high cost (Torkaman et al., 2016).

Immutability: The blockchain permanent ledger feature drives the core advantage of integration to IoT. This way, data entered by the users' nodes can't be modified once the nodes confirm and verify the data (Vilchez, et al., 2023; Nakamoto, 2008). Ensuring that data entered are stored and kept safe is a crucial improvement for the current IoT technology, improving security and privacy.

Anonymity: In order to process transactions or data exchange in a blockchain network, nodes involve using unique anonymous address numbers that hide their identities. If this approach is employed in IoT and used for other purposes, such as a voting system, it can be an advantage (Rejeb et al., 2023; Nakamoto, 2008).

Blockchain's built-in security features, such as its resilience to cyberattacks and robust cryptographic safeguards, mitigate the vulnerabilities often present in diverse IoT environments, increasing trust among developers in its potential applications. The technology's efficiency and cost-effectiveness also contribute to the economic viability of IoT networks in Malaysia, where budget constraints are common. Additionally, Blockchain's immutability and ability to ensure privacy significantly improve data integrity and address privacy concerns, which are critical to IoT stakeholders. These advantages promote greater trust and regulatory compliance, supporting the hypothesis that Blockchain's perceived usefulness positively impacts the development of Malaysia's IoT ecosystem. Collectively, these benefits demonstrate Blockchain's transformative role in advancing the nation's IoT landscape. Thus, the following hypothesis is proposed to answer the first research objectives.

H_1: There is a positive relationship between the perceived usefulness of Blockchain technology and the IoT ecosystem in Malaysia.

2.9.2 Awareness of Blockchain to IoT within IoT Developers

The significance of blockchain has been likened to that of the Internet in the early 1990s, owing to its vast array of advantages across various sectors (Casino et al., 2019). Blockchain is widely recognized as a transformative force, with the potential to drive digitization in nearly all areas involving value exchanges (Dutta et al., 2020). Developed nations are already harnessing the benefits of blockchain, its impact on the socioeconomic landscape of developing countries, particularly in governance, education, healthcare, and business, is substantial ((Bazel et al., 2021).

In Malaysia, however, blockchain has not advanced significantly, primarily due to the absence of structured frameworks and a general lack of awareness (Bazel et al., 2023). According to the Malaysian Industry-Government Group for High Technology (MIGHT), blockchain is anticipated to gain traction across various domains in Malaysia by 2025. Local banks, such as CIMB and Maybank, are actively promoting the awareness of this technology, with MIGHT confident that blockchain will enhance productivity and transparency in multiple sectors (MIGHT, 2019). The national Applied Research and Development Centre (MIMOS) is committed to advancing blockchain as part of Malaysia's digital transformation initiative. Blockchain is seen as a key engine for this transformation, supported by five foundational ecosystem elements: Collaboration, Amplification, Talent, Legal and Governance, and Enablers. Noteworthy applications of blockchain in Malaysia include projects focused on palm oil traceability, contactless payment tracking, and vaccination record management (MIMOS, 2021)

Despite blockchain potential advantages, several awareness challenges must be addressed to fully realize the benefits of blockchain. The National Blockchain Roadmap 2021-2025 aims to prepare Malaysia for the next phase of blockchain development, extending beyond Bitcoin. This roadmap seeks to tackle issues such as fraud management, supply chain monitoring, and identity verification to improve efficiency and reduce costs (Bazel et al., 2023). Blockchain is poised for acceptance and adoption due to its seven compelling features that address critical business concerns across various sectors: security, time and cost efficiency, fraud reduction, record keeping, decentralization, transparency, and smart contracts.

In response to the Malaysian government's call for an increase awareness within the blockchain domain (Bazel et al., 2024), it is essential to conduct studies that provide a comprehensive overview of the existing body of knowledge in this area. Currently, there is a lack of studies or thorough evaluations detailing the state-of-the-art developments in Malaysia's blockchain landscape. Thus, the following hypothesis is proposed to answer the second research objectives

H_2: There is a positive relationship between the awareness of Blockchain technology and the IoT ecosystem in Malaysia

2.9.3 Adoptability Rate of Blockchain with IoT within the Ecosystem

The adoption of blockchain technology has been extensively examined across various sectors, including supply chains (Chowdhury et al., 2023; Agi & Jha, 2022; Jung, 2022), logistics (Alazab et al., 2021; Park, 2020), banking(Hashimy et al., 2023; Cho et al., 2023; Jena, 2022), accounting and auditing (Palos-Sanchez et al., 2021; Fülöp et al., 2022), e-commerce systems (Ferri et al., 2021), tax administration (Shrestha et al., 2021), educational frameworks (Queiroz et al., 2021), and construction (Li et al., 2022; Cheng & Chong, 2022), among others (Pham & Nguyet, 2023; Bakri et al., 2023; Malik et al., 2022; Dehghani et al., 2022). However, there exists a notable deficiency in research focusing specifically on the adoption of blockchain within the software development industry in Malaysia content, including the factors influencing adoption and the frameworks available for implementation, as highlighted in previous studies of Nazim et al., (2021). This gap is particularly concerning given the critical role software companies play in contemporary business ecosystems.

As of April 2020, Malaysia was home to 48 blockchain startups, significantly fewer than Singapore's 397 (Tracxn, 2021). This disparity can largely be ascribed to a shortage of local expertise in blockchain development (Yunus & Jalil, 2019). In addition to a deficiency in cryptography skills necessary for advancing blockchain technology, there exists a general lack of awareness regarding its potential benefits. While public understanding of blockchain is crucial, businesses themselves must also become more informed to leverage the technology effectively.

To advance in the blockchain sector, Malaysia could benefit from attracting foreign firms to establish regional hubs. For instance, Chaintope Inc. has recently revealed plans to develop its Malaysian subsidiary, Chaintope Malaysia, into a Southeast Asian hub focused on sustainability projects utilizing blockchain technology (The Star, 2021). Factors contributing to this decision include Malaysia's stable environment, availability of proficient English-speaking talent, and cost efficiency compared to other countries in the region.

In Malaysia, three primary industries exploring blockchain applications are renewable energy and utilities, palm oil and agriculture, and Islamic banking (Sharon, 2018). Notable recent blockchain initiatives include the collaborative launch of digital vaccination certificates for Covid-19 vaccine recipients (Bernama, 2021) and the implementation of traceability systems in the palm oil sector by the Malaysian Palm Oil Council (Neo, 2020). Both of these projects are large-scale and necessitate substantial financial investment.

Moreover, the halal food market presents another significant opportunity for blockchain application. While the global halal food market is experiencing robust growth, Malaysia currently captures only 1% of global demand (Mohtar, 2020). Implementing blockchain technology in this sector could enhance transparency and trust, thereby mitigating issues related to scandals that have emerged in recent years.

The existing body of literature indicates significant potential benefits of blockchain technology, such as enhanced efficiency and improved security, which are well-documented in various fields. Yet, the absence of studies addressing the software sector underscores a crucial research void. Further exploration into blockchain adoption among software firms could illuminate their preparedness for this technology and the determinants affecting their adoption choices. Such insights would be invaluable for software developers contemplating the integration of blockchain technology, enabling them to leverage its advantages effectively.

H_3: There is a positive relationship between the adoption rate of Blockchain technology and the IoT ecosystem in Malaysia

2.10 Conceptual Framework

The overall strategy for conducting research is referred to as research design. Through data gathering, interpretation, analysis, and discussion, the general method presents a simple and realistic plan to solve sustainability research challenges (Robson, 2002).

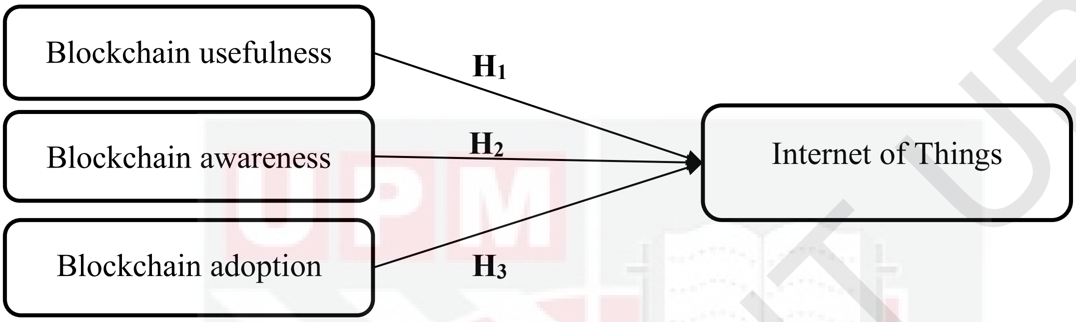

Figure 2.3 : Research Conceptual Framework

Hypothesis

H_1: There is a positive relationship between the perceived usefulness of Blockchain technology and the IoT ecosystem in Malaysia

H_2: There is a positive relationship between the awareness of Blockchain technology and the IoT ecosystem in Malaysia

H_3: There is a positive relationship between the adoption rate of Blockchain technology and the IoT ecosystem in Malaysia

2.10.1 Analysis of the Hypothesis (Inferential)

Inferential statistics is a subfield within the discipline of statistics that utilises analytical methods to make inferences about a population based on data obtained from representative samples. Inferential statistics are utilised to make inferences regarding a population, which serves as the primary objective of any inquiry. In the field of inferential statistics, a statistic is computed based on the data collected from a sample, and afterwards employed to make inferences about a parameter that holds significance for the full population. By utilising data obtained from representative samples, inferential statistics provide insights into the broader population. Inferential statistics are derived by an examination of the normalcy of the underlying data. The primary research data undergoes a normality test in order to determine if it adheres to a normal distribution, which is essential for the statistical evaluation of the study's findings. The study conducted on the primary data will be rigorous, taking into consideration the results of the normalcy test. A diverse range of analytical tests and methodologies enable researchers to enhance the precision of their population-level generalisations.

2.10.2 Normality Test

Prior to conducting any statistical analysis, it is imperative to assess the normality of the data, as this enables the researcher to select the right statistical test (Clason & Dormody, 1994). According to Clason and Dormody (1994), a considerable body of research has emphasised the importance of utilising analytical methods and methodologies that assume normal distribution in data analysis. In contrast, it is often the case that data is not commonly dispersed. There exists a variety of statistical analytic tools that can be employed to evaluate the normality of data, including but not limited to box plots, measures of skewness and kurtosis, the Kolmogorov-Smirnov test, and histograms. In empirical datasets, it is commonly seen that data do not adhere to a specific distribution. In such instances, researchers often resort to employing non-parametric tests as a means of analysis (Lantz, 2013). According to Peat and Barton (2005), the Kolmogorov-Smirnov test is known for its high sensitivity to outlying values. However, the application of the Lilliefors correction helps to mitigate this issue, making the test more moderate in its results.

Table 2.1 : Result Assessment of Data Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
AUBT	.198	250	.000	.869	250	.000
AALE	.174	250	.000	.881	250	.000
AYO	.153	250	.000	.906	250	.000
ABIE	.125	250	.000	.927	250	.000

a. Lilliefors Significance Correction

According to Thode (2002), the validity of the Kolmogorov-Smirnov test has been found to be inadequate hence caution should be exercised when using it to assess the normal distribution of a sample. According to Steinskog (2007), employing a substantial sample size is not recommended for the purpose of parameter estimation. The Shapiro-Wilk test is known to possess greater statistical power compared to the Kolmogorov-Smirnov test, particularly when the Lilliefors correction is taken into consideration (Steinskog, 2007). The power of the Shapiro-Wilk test in assessing deviations from predicted normality in a sample is frequently employed as a measure (Thode, 2002). The Shapiro-Wilk test is frequently referenced as the preferred method for assessing the conformity of data to a normal distribution.

Table 2.2 : Research Test and Analysis Methods

There is a positive relationship between		Analysis Type
H_1	The usefulness of Blockchain with IoT ecosystem	Spearman
H_2	The awareness of Blockchain to IoT within IoT developers	Correlation &
H_3	The adoptability rate of Blockchain with IoT within the ecosystem	Ordinal Regression

The results of the Kolmogorov-Smirnov and Shapiro-Wilk normality tests, which are widely used in statistical analysis, are presented in Table 2.1. The Shapiro-Wilk test is commonly advised for datasets containing less than fifty observations. However, the test has the capability to process data samples up to a maximum of 2000 samples. Consequently, the Shapiro-Wilk test is utilised as a quantitative method to evaluate the normality of the data gathered in this research. The results of normality tests indicate that the data obtained from participants does not follow a normal distribution, as evidenced by the p-value of .05 for all items within the three variables under investigation in this research. When the p-value of the Shapiro-Wilk test exceeds 0.05, it is generally accepted that the underlying data can be considered to have a normal distribution. This discovery implies that it would be advisable to do a non-parametric analysis. The hypothesis and analysis techniques of the study are succinctly presented in Table 2.2.

2.10.3 Non-parametric Analysis

Non-parametric testing refers to a statistical analysis approach that does not rely on preconceived assumptions about the distribution of the data being tested, particularly when the data does not follow a normal distribution. Non-parametric tests are alternatively referred to as non-distributed tests due to this characteristic. Parametric tests, such as the T-test or analysis of variance, are applicable only under certain conditions and assumptions regarding the underlying data. In cases where these criteria are not met, non-parametric tests can be employed as an alternative. The data collected and analysed for this study deviates from a normal distribution. Therefore, the Spearman correlation and ordinal regression analyses are employed.

2.11 Summary

This chapter offers a thorough review of existing literature on the integration of Blockchain technology with the IoT, focusing on its potential applications, challenges, and impact within Malaysia's IoT ecosystem. It begins by examining the current state of IoT infrastructure, characterized by a reliance on centralized server-client models. This reliance creates challenges in scalability, security, and costs as IoT networks expand, underscoring the need for more robust and decentralized solutions.

The review then delves into Blockchain technology's capabilities, such as its decentralized architecture, data immutability, and use of smart contracts. These features collectively enhance data security, privacy, and operational efficiency within IoT networks. By decentralizing data management and removing single points of failure, Blockchain offers promising solutions to IoT's limitations, including centralization bottlenecks and interoperability issues. Nevertheless, the chapter also discusses existing knowledge and implementation gaps in Malaysia, where Blockchain's integration with IoT is still emerging, hindered by limited awareness, regulatory barriers, and a lack of familiarity among key stakeholders.

To provide a broader context, this chapter incorporates studies on the perceived usefulness, awareness, and adoption trends of Blockchain across various sectors worldwide, particularly focusing on IoT applications. Through synthesizing this literature, it becomes clear that understanding Blockchain's role in enhancing IoT—especially regarding security, scalability, and interoperability—will be crucial for Malaysia's evolving IoT ecosystem.

CHAPTER 3

RESEARCH METHODOLOGY

This chapter describes the methods that will be used to conduct the research. In addition, this chapter introduces the research design, research approach, source of data, survey instruments, data collection techniques, research area and population, population samples and unit of analysis, sampling techniques, data analysis procedures, and summarises the study of the pilot research result.

3.1 Research Design

The overall strategy for conducting research is referred to as research design. Through data gathering, interpretation, analysis, and discussion, the general method presents a simple and realistic plan to solve sustainability research challenges (Robson, 2002). Quantitative research will be used in this study. Quantitative research is a formal, objective, and systematic method of obtaining numerical data on any subject (Burns, 2005). The research methods deal with getting outcomes by measuring and analysing variables, which entails using and analysing numerical data to answer questions using specialised statistical approaches (Apuke, 2017). Other researchers described this research project to describe phenomena by collecting numerical data analysed using mathematical methods (especially statistical methods) Aliaga et al., (2006). Furthermore, the quantitative research design can help researchers explain and test relationships and study causal relationships between variables. That is to say, the design of this type of study allows researchers to test the study's hypothesis (Coolican et al., 1990).

3.2 Research Approach

There are three types of approaches in general: deductive, inductive, and abductive (Saunders et al., 2003; Kitchenham et al., 2007). The method adopted in this study is a deductive one. The deductive method examines the validity of current hypotheses (or theories/hypotheses), whereas the inductive method aids in developing new ideas and generalisations. On the other hand, the abductive approach is based on compelling inquiry, which begins with a "surprising fact" or "puzzles questions," and the inquiry process is specialised and dedicated to their explanations. (Bell et al., 2018; Luo, 2021). The deductive approach can be described as scientific research, usually based on quantitative data. Thus, the deductive approach is typically related to quantitative research, while the induction approach uses qualitative data.

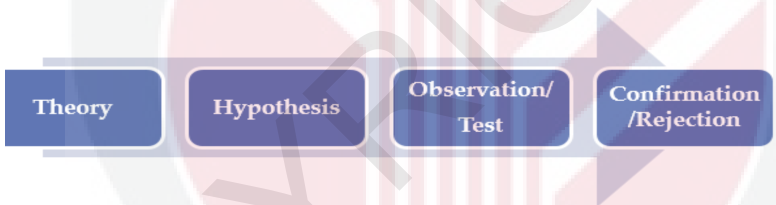

Figure 3.1 : Deductive Approach Process

Conversely, the deductive approach develops theory or conceptual structure and then empirically tests (Creswell, 2013). That is to say; the deductive approach involves adopting a general theoretical framework and testing it under specific circumstances. For example, in Creswell et al. (2007), the researchers state that one can use existing theories to formulate hypotheses. In this case, these assumptions are formed using theories that already have facts to observe and confirm whether current theories are accepted or rejected.

3.2.1 The Qualitative and Quantitative Approach

The primary objective of utilizing qualitative research methods is to obtain a holistic understanding of human experiences within their broader context. Qualitative research emphasizes the importance of verbal narratives, individual accounts, and detailed descriptions, rather than relying on numerical data. This approach allows for a deeper exploration of phenomena, free from the constraints of predefined hypotheses or rigid theoretical frameworks. In contrast to quantitative research, which often begins with formulated hypotheses, qualitative inquiry typically generates hypotheses or theoretical insights following the collection and analysis of data. This methodology offers a unique opportunity to understand how individuals interpret and adapt to their environments over time, providing an in-depth examination of behaviors, motivations, and interactions within social contexts (Gautam & Gautam, 2023).

Quantitative research, as characterized by Sekaran and Bougie (2016), focuses on the collection and statistical analysis of numerical data. This approach is cantered on gathering measurable data that can be immediately analysed, facilitating the testing of hypotheses and the formulation of generalizable conclusions. In contrast to qualitative methods, quantitative research is particularly useful for identifying patterns and relationships within data, and it often aims to establish objective, verifiable results. This thesis adopts a quantitative research methodology to systematically assess the relationships between key variables, specifically the usefulness, awareness, and adoptability of blockchain technology into the IoT ecosystem.

This research method is grounded in deductive principles and aligns with the naturalistic scientific perspective emphasized by Treagust and Won (2023). It underscores the significance of empirical data in establishing causal relationships. Given the specific nature of the research questions and the need for comprehensive statistical analysis, a quantitative approach is deemed essential for this study. This methodology facilitates the systematic collection and analysis of data, ensuring that the study's conclusions are both robust and applicable within the broader context of the Malaysian IoT development landscape.

Table 3.1 : Qualitative and Quantitative Approach Basic Differences

S/N	Qualitative	Quantitative
1.	Put into words	Put simply with the numbers.
2.	Minimal data set	A larger number of subjects
3.	Open-end questions	Close-end questions
4.	Find new ideas	Prove the theory

(Source: Bryman and Bell, 2011)

In Table 3.1, a comparative overview of the distinguishing characteristics of qualitative and quantitative research methodologies, illustrating why the latter is most suitable for addressing the research objectives is depicted. By adopting this approach, the study will effectively assess hypotheses related to the usefulness, awareness, and adoptability of blockchain technology within the IoT ecosystem in Malaysia.

3.3 Data Collection

Data collection plays a significant role in statistical analysis. Researchers rely on two types of data sources to conduct research, namely primary and secondary data sources (Bourn, 2019). This study will use the primary data source. The primary data source is the original data source, the source of data collected first-hand by researchers for specific research purposes or projects. This primary data can be collected in a variety of ways. However, the most common techniques are interviews, questionnaires, field observations and experiments. The primary data is not yet published and is more authentic, reliable, as well as objective. Furthermore, humans do not modify or change the original data; therefore, its effectiveness is more significant than secondary data. Thus, the primary data of this study will be collected in the form of a questionnaire.

3.3.1 Study Location

As defined in (Penrod et al., 2003; Churchill et al., 2002), the study location is the sum of all people that fit into a set of norms or specifications that cover the entire population of interest to which the researchers' results can be generalised. However, the research study location is limited to Malaysia. Sekaran et al. (2013) explain that population refers to the events or impacts that researchers want to explore in the entire study location. Therefore, the population of this study is based on all IoT players in Malaysia, who are key actors in the ICT and IT industry that uses IoT and blockchain in any form.

The present study acquires data regarding the IoT players in Malaysia from the human resources departments of said companies. The researcher then proceeds to randomly select developers from the provided list till the necessary sample size is achieved. The present study utilises a simple random sampling technique. The utilisation of a simple random sampling strategy was favoured in order to enhance the overall generalizability of the research findings, as it guarantees a high level of representativeness within the selected sample.

3.3.2 Sample Technique

According to Sekaran and Bougie (2010), the utilisation of a simple random sampling technique contributes to the improvement of result generalizability to the entire population, as it ensures the inclusion of all aspects within the population. Every individual element possesses an equitable probability of being selected as the subject. According to Collis and Hussey (2009), the utilisation of random sampling techniques can effectively mitigate sampling error by ensuring that each unit within the population has an equal and independent opportunity to be selected as a subject. Therefore, the utilisation of random sampling is favoured due to its statistical efficacy in mitigating potential sample errors, and is deemed appropriate for this study due to its distinctiveness in comparison to other methodologies employed in previous research endeavours. A number of researches examined in this study employed a simple random sampling technique. Nevertheless, one notable drawback associated with the utilisation of the basic random sampling technique is the inherent difficulty and time-intensive nature of its implementation.

3.3.3 Study Population and Sample Size

A population refers to a clearly delineated group of humans or items that have common characteristics. Hence, the focus of this study encompasses ICT and IT industry players that use IoT and blockchain in any form located in Malaysia. The population size of registered active ICT and IT industry players in Malaysia, is 2708 (as of December, 2021 by MDEC). A sample of 101 companies will be selected for the distribution of questionnaires. Simultaneously, the scope of examination encompasses developers employed by ICT and IT firms, as succinctly presented in Table 3.2.

Table 3.2 : Study Unit of Analysis

Job Level	Number of respondents
Blockchain Developers	230
IOT Developers	260
Total	**490**

The researcher chooses to pick the target population in order to examine the correlation between usefulness of Blockchain, awareness of Blockchain, and adoptability rate of Blockchain with IoT ecosystem practices in Malaysia. In order to accomplish the study's objectives, a survey will be administered to a sample of 349 participants drawn from a pool of ICT and IT firms that have been specifically chosen for this study. The study sample size is determined using the Yamane (1967) formula, as depicted below.

$$n = \frac{N}{1 + N * e^2} = \frac{2708}{1 + 2708 \times 0.05^2} = 348.5 \;\cong\; 349$$

Where n= Required Sampling size, N= Population Size, e= Acceptable Error (0.05), and c= Confidence Level (0.95). Based on the acquired sample size, the researcher would employ the minimum sample size to ascertain the suitable number of oversamples. Fink (2017) delineated a two-step procedure for researchers to employ when utilising oversampling approaches for sample size distribution. The initial phase of the procedure involves the determination of the minimum required sample size. After establishing the lowest sample size, the researcher proceeds to compute the required number of additional individuals to be added in order to constitute a representative sample. Salkind (1997) argues that a 40-50% oversample is necessary to account for anticipated survey non-response, missing data, and uncooperative participants. Therefore, the participants of the study were oversampled by 40%, as seen in Table 3.1.

$$OS = n * \ 0.40 = 349 * 0.40 = 488.6 \ \cong \ 489$$

In the present context, the value "0.40" denotes the complete augmentation beyond the initial sample size, equivalent to a 40% increment. In order to optimise the probability of obtaining a comprehensive answer, a total of 489 developers from the selected ICT/IT firms will be requested to complete the survey. In addition, the sample size is justified by the Krejcie and Morgan (1970) sample, as shown in Table 3.3. The determination of the appropriate sample size is contingent upon the characteristics of the population under investigation within a specific environment, as well as the objectives and goals of the research endeavour. Insufficient or excessive sample sizes might compromise the primary objective of a study and result in increased expenses and insufficient resource allocation. Hence, it is imperative that the sample size adheres to optimal standards, avoiding both excessive smallness and largeness (Kothari, 2004). Sample size determination is influenced by various aspects, such as cost, statistical analysis methodologies, previous research studies on the topic, and the nature of the research (Bryman and Bell, 2011). Please see appendix A for the comprehensive compilation of the chosen registered companies.

Table 3.3 : Classification Criteria Sample Size Data Collection

Number Range	Classification	Number Range	Classification
Below 50	Very Weak	301 – 500	Very Good
51 – 100	Weak	501 – 1000	Excellent
101 – 200	Adequate	1001 above	Very Excellent
201 – 300	Good		

(Source: Krejcie and Morgan 1970)

Additional criteria taken into account throughout the process of selecting the sample size include the financial resources at hand and the temporal constraints associated with conducting the study. According to Bryman and Bell (2011), it is recommended to select a sample size that is manageable in order to effectively reflect the population, hence optimising time and cost efficiency. The sample size employed in this study is deemed sufficient and distinctive in relation to the existing body of research.

3.3.4 Data Collection Method

The data collected will come from the questionnaire. This process will be carried out in several stages, including the development of the questionnaire, determining the area and location where the questionnaire will be distributed in groups, distributing the questionnaire to selected respondents, and randomly reminding the respondent of the deadline of the questionnaire, the questionnaire collection and data analysis. For the purpose of this research, a questionnaire will be used because it is easy to do, and much information can be obtained from a large number of respondents. When researchers target large numbers of people, online questionnaires can also help reduce costs. The response received is always frank and anonymous. Compared to interviews, questionnaires are very suitable for sensitive and self-related questions. It takes less time to use the questionnaire to conduct a survey, and the respondent can also fill in the questionnaire at the appropriate time. Once the data is collected from the respondent, the researcher will take initial steps to conduct inspections and error checking to ensure that the data is ready for further analysis, including:

3.3.5 Data Cleaning and Coding

This is the process of checking raw data to identify possible errors and omissions during data collection or sampling (Kothari et al., 2014). This study uses this to improve data accuracy by checking for omissions, such as blank answers in the questionnaire, varying answers, etc. the data coding process is a way of identifying and classifying each response using symbols (Awang et al., 2012) or numerical scores. In (Cheng et al., 2014), the researcher stated that this process in which quantitative (such as questionnaire survey results) and qualitative (such as interview records) data are classified to facilitate analysis. One of the purposes of coding is to convert data into a form suitable for computer-aided analysis. Therefore, after the original or raw data editing and cleaning process, the data of this study are numerically coded. During the coding process, the researchers checked every question and every answer to reducing confusion.

3.3.6 Dealing with Missing Responses during Data Entry

This involves entering code data directly into the software, allowing researchers to convert the raw data into appropriate information. SPSS software will be used in this research, and an error editing routine will be developed to detect data entry errors. The eye-scanning process will also be used in the study to minimise data entry errors. Sekaran and Bougie (2016) assert that the predominant method employed in social science research is the utilisation of questionnaires. According to Zikumnd et al. (2003), a significant number of questions may be left incomplete when the survey is administered manually. Hence, the occurrence of missing values is a prevalent concern in the process of data processing (Tabachnick & Fidell, 2007). Missing values occur when respondents choose not to respond or fail to respond to one or more items. The absence of these responses poses challenges in the process of quantitative data analysis, as it leads to a decrease in the sample size due to non-response, hence diminishing the statistical power.

The presence of multivariate analytic issues is a consequence of this phenomenon (Hair et al., 2014). However, the data that is not present can be classified into two distinct categories: 'ignorable' and 'not-ignorable.' In instances where missing data cannot be ignored, such values can arise due to technical problems on the part of the investigator, such as errors in data entry, or due to respondents choosing not to answer or failing to provide complete information. Moreover, the category of missing data that can be disregarded does not necessitate any intervention for its handling, and it may even be intentionally included as a component of the survey instrument. In the context of this study, it is important to note that no instances of missing data were identified within the entirety of the dataset. This may be attributed to the utilisation of a Google form that enforced compulsory completion, hence ensuring comprehensive data collection.

3.4 Instrument/Questionnaire Development

As a component of the research methodology employed in this study, surveys are planned to be administered to developers working in ICT/IT firms located in Malaysia. The researchers intend to assess the reliability and validity of a variable measure of Blockchain usefulness, awareness, and adoptability rate with the IoT ecosystem practices by conducting tests using a 27-item scale. The selection of the questionnaire as the data measurement instrument was based on multiple factors. Initially, the selection of a questionnaire as the data collection method was predicated on its capacity to efficiently gather a substantial volume of data within a limited timeframe. Additionally, the selection of a questionnaire was based on its cost-effectiveness. This suggests that the questionnaire has the capability to gather large amounts of data at a comparatively lower cost. In addition, the selection of a questionnaire as the research instrument was based on its ability to provide respondents with the flexibility to complete the questions at their own leisure (Collis and Hussey, 2009). The questionnaire serves as a tool for gathering essential primary data. The questionnaires were affixed to a cover letter that provided an explanation of the survey's aim and objectives. The questionnaire is organised into distinct sections, each including a total of 27 closed-ended questions, with three sections A, B, and C. The survey has a set of five closed-ended questions that pertain to the study dependent and independent variables.

3.4.1 Demographic Variable

By utilising an adjusted seven-item nominal scale survey, the researcher is able to ascertain the fundamental worth of the participants' "demographic" information. The fist portion, labelled A, encompasses the demographic profile of the respondents. This includes information such as the age, gender, work position, education level, work tenure firm sector and enterprise size.

Table 3.4 : Demographic Information

Measurements	No. of Questions
Demographic Questions	7

3.4.2 Dependent Construct (IoT)

The questions created comprises five (5) items that assess the developer's grasp of IoT in relation to Blockchain usefulness, awareness, and adoptability rate.

Table 3.5 : IoT

Measurements	No. of items
Blockchain can accelerate IoT tamper-proof	
Blockchain can accelerate IoT autonomy	
Blockchain can accelerate IoT robust level of encryption	5
Blockchain can accelerate IoT node's reliability	
Blockchain can accelerate IoT big data transparency and analysis	

3.4.3 Independent Construct (Usefulness, Awareness and Adoption)

On the next part of the scales, this questionnaire comprises a total of ten (15) items. The initial five (5) items pertain to usefulness, the second five (5) items measure the awareness, while the subsequent five (5) items address adoption variable.

Table 3.6 : Usefulness, Awareness and Adoption

Measurements	No. of items
USEFULNESS	
Blockchain decentralised feature has no single point of failure	
Blockchain have better data security and privacy	5
Blockchain provide better transparency and traceability	
Blockchain has increased efficiency and reduced costs	
Blockchain technology permit data verify without need for third-parties	
AWARENESS	
Are you aware of centralised and decentralised distribution systems?	
Are you aware of blockchain, smart contracts, edge computing and IOT?	
Are you aware of blockchain use in IOT?	5
Are you aware of smart contract use in IOT?	
Are you aware of blockchain use for data management?	
ADOPTION	
Does the subject of blockchain have any role to play in data management	
Does blockchain have any role to play in data security and privacy	
Is big blockchain, smart contract and IOT related to each other	5
Blockchain is helpful in increasing IOT data security and management	
Will recommend blockchain technology to management of your company	

The metrics utilised in this study were derived from other research endeavours that investigated analogous variables within a different setting. The study employed a process of adaptation and modification of questions derived from prior research endeavours. The measurement scale for all constructs is presented in Table 3.7, where the participants are requested to express the level of usefulness of Blockchain, awareness of Blockchain, and adoptability rate of Blockchain with IoT ecosystem practices and techniques during the last three-year period. The researchers utilised a 5-point Likert scale to assess the dependent and independent variable with the following response options: 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, and 5 = strongly agree. The researchers opted for the utilisation of a 5-point Likert scale due to its inherent advantages, which afford participants greater flexibility in expressing their opinions and preferences. This scale facilitates a clear and unambiguous selection of responses, hence enabling researchers to efficiently gather and analyse the collected data. Please refer to Appendix 1 for a comprehensive description of the questionnaire.

Table 3.7 : The Items for Measuring All Dependent and Independent Variable

Variables	Modified Question for this research	Source
Blockchain	Blockchain can accelerate IoT tamper-proof Blockchain can accelerate IoT autonomy Blockchain can accelerate IoT robust level of encryption Blockchain can accelerate IoT node's reliability Blockchain can accelerate IoT big data transparency and analysis	Khan et al., 2021; Dubey et al., 2020
Usefulness	Blockchain decentralised feature has no single point of failure Blockchain have better data security and privacy Blockchain provide better transparency and traceability Blockchain has increased efficiency and reduced costs Blockchain technology permit data verify without need for third-parties	Ammar et al., 2023; Kamble et al., 2019
Awareness	Are you aware of centralised and decentralised distribution systems? Are you aware of blockchain, smart contracts, edge computing and IOT? Are you aware of blockchain use in IOT? Are you aware of smart contract use in IOT? Are you aware of blockchain use for data management?	Ammar et al., 2023; Sciarelli et al., 2022
Adoption	Does blockchain have any role to play in data security and privacy Is big blockchain, smart contract and IOT related to each other Is big blockchain, smart contract and IOT related to each other Blockchain is helpful in increasing IOT data security and management Will recommend blockchain technology to management of your company	Garg et al., 2021; Esfahbodi et al., 2022

3.4.4 Instrument/Questionnaire Validity Test Method

Content and validity testing will be performed on the survey instrument to guarantee that it can measure what needs to be measured and if the elements appear relevant, clear, and essential. Thus, content validity refers to academia's independent evaluation of the appearance and relevance of the instrument used for assessment. In addition, when attempting to assess a phenomenon, content validity determines if the content of the questionnaire or item measured with the instrument is representative and sufficient. Some survey questions asked in the instrument have nothing to do with the planned test subject; it could be stated. To better understand the consistency between evaluators and raise confidence in the effectiveness of the new instrument content, Brennan and Hays (1992) advised that both proportional consistency and data variability indicators be utilised. In addition, the researchers will consult various specialists in the field of research with a smaller sample size to provide information on the size of the structure and research components to best suit the research objectives. Finally, the survey participants will be asked to score the questionnaire's quality in terms of relevance, clarity, and necessity.

Table 3.8 : Content Validation Index Scale

Scale	1	2	3	4
Relevant	Not relevant	Somewhat relevant	Quite relevant	Very relevant
Clarity	Not clear	Needs revision	Clear but need revision	Very clear
Essential	Not essential	Somewhat essential	Useful but not essential	Essential

To help validate the questionnaire, the researcher seeks the assistance of four specialists, each possessing a minimum of five (5) years of experience in the ICT/IT industry as IoT or Blockchain developer, in order to authenticate the questionnaire. The validation form is created with Google Forms and shared with them online to ensure that the questions adopted and produced are relevant, clear, and vital. The minimum number of validators for content verification is 2, but most suggestions propose at least 5 - 10 validators. The number of validators checking the content should be at least five (5) and no more than 10 based on the recommendations and experience of the reference author (Lynn, 1986). As a result, the total number of validators to be used for this questionnaire content validation is 5. Table 3.8 shows above the validation scale in its entirety. The overview of the recommended number of validators participating in the Content Validity Index (CVI) and the CVI's acceptable cut-off score is presented in Table 3.9.

Table 3.9 : The Number of Validators and Its Implication on the Acceptable Cut-off Score of CVI

No. of validators	Acceptable CVI values	Source of recommendation
2	At least 0.90	Davis (1992)
3 - 8	At least 0.83	Polit & Beck (2006) Lynn (1986)
9 - 10	At least 0.78	Lynn (1986)

3.4.5 Validity Test Result

Table 3.8, located above, row 2, offers a concise overview of the recommended quantity of validators to engage in the Content Validity Index (CVI), along with the acceptable threshold score for the CVI. Furthermore, according to the calculations provided in Table 3.10, it can be inferred that the I-CVI, S-CVI, and S-CVI/UA have all achieved a sufficient level for the total number of validators employed.

Table 3.10 : Validators and CVI Cut-Off Score Result

Scale	T. A	S-CVI	S-CVI/UA	No. of validators	Acceptable CVI
Relevant	28	0.98	0.92		
Clarity	27	0.97	0.89	5	At least 0.83
Essential	29	0.99	0.96		

For the relevance of the questions, a total of 28 validators were in agreement, with an S-CVI of (0.98) and an S-CVI / UA of (0.92). Although a capacity of 27 validators agreed on the clarity and essentiality of the questions, clarity S-CVI holds at (0.97), S-CVI / UA at (0.89). This measure also did not hold for the essentiality, which the S-CVI and S-CVI / UA computed values at (0.99) and (0.96), respectively. This finding suggests that the pre-test questionnaire has demonstrated a satisfactory degree of content validity. The questionnaire is now ready for implementation in a pilot study aimed at assessing the respondents' comprehension and ability to effectively respond to the questions.

3.4.6 Pilot Study

Before the researcher generates the data for this study, the researcher needs to conduct a pilot study to ascertain the credibility of these questions designed if they are suitable for the respondents and provide the instrument's validity. Zikmund (2003) defined a pilot study as a trial run with a group of respondents to screen out problems in the instructions or design of a questionnaire'. The advantages of the pilot study in survey questionnaires have long been recognized by researchers (Churchill et al., 2005; Emma et al., 2018; Hunt et al., 1982) to ensure that respondents can comprehend all questions with no ambiguity and no troubles related to wording or measurement.

Table 3.11 : Acceptable Level of Coefficient for Reliability

No.	Cronbach's Alpha coefficient	Remark
1.	Below .70	Substandard
3.	Between .70 and .90	Satisfactory
5.	Much above .90	Very Satisfactory

(Source: DeVellis, 1991)

Therefore, to determine the underlying dimensions of the construct and ascertain the internal validity, a pilot study will be conducted to check on the reliability and validity of the instrument. The suggestions for improvement obtained from the pilot test respondents will be incorporated in the final questionnaire, and 50 respondents will be selected as the pilot test respondents. The pilot study holds significant importance in research as it focuses on evaluating and enhancing the questionnaire by assessing the instruments obtained from the respondents (Rasinger, 2013).

Prior to completing the main field study, a preliminary pilot study was conducted to ascertain that all the measured variables exhibited a minimum reliability coefficient of 0.7 or above. The study conducted by Habsahet et al. (2018) showed that the pilot study findings were deemed important, acceptable and credible. According to Tseng and Sim (2021), it is often advised to utilise a sample size that constitutes 10 to 20% of the overall sample size employed in the comprehensive survey, or a minimum of 30 to 50 participants. Therefore, Table 3.12 presents the reliability test conducted by the researcher for a preliminary study using a sample of fifty (50) questionnaires collected from IoT and Blockchain developers in distributed ICT/IT firms. The aforementioned procedure was undertaken in order to ascertain the dependability and accuracy of the questionnaire prior to its ultimate dissemination.

Table 3.12 : Pilot Study Reliability Results (50 Participants)

Constructs	No. of items	Cronbach's Alpha	Remark
Usefulness	5	.916	Acceptable
Awareness	5	.856	Acceptable
Adoption	5	.864	Acceptable
Blockchain	5	.960	Acceptable

The process involved the validation of the questionnaire, which served as the instrument. Experts with a minimum of 2 years of experience in the ICT/IT firms, specifically in roles such as developers, were engaged to enhance the questionnaire's reliability and validity in assessing Blockchain importance within IoT services firms. According to Joshi et al. (2015), conducting a pilot study is essential for determining the feasibility of future investigations and informing researchers on whether to proceed with the proposed study. Additional elucidations additionally demonstrate that a pilot investigation functions as a mechanism for assessing the coherence and dependability of items or constructs, and is executed on a reduced scale compared to the substantive field study. Nevertheless, the administered questionnaire demonstrated that the constructs and items in issue exhibited a reliability coefficient over 0.70, establishing their reliability and appropriateness for subsequent investigation within the scope of this study.

Additionally, the Cronbach alpha coefficients for the constructs IoT, usefulness, awareness and adoption of blockchain ranged from **0.856 to 0.960**, as determined from a sample of 50 participants in the pilot study. This finding provides more evidence supporting the reliability and acceptability of the tool. Consequently, all of the items and constructs exhibited a satisfactory level of 0.70 or above, thus justifying the implementation of the empirical investigation. Whereas table 3.13 presents the correlation analysis outcomes and comprehensive statistical information pertaining to the examined questions. This includes the Pearson Correlation coefficient and the significance level (two-tailed) for all constructs.

Table 3.13 : Pilot Study Results (50 Respondents)

		Usefulness	Awareness	Adoption	Blockchain
Usefulness	Pearson Correlation	1	.770**	.699**	.725**
	Sig. (2-tailed)		.000	.000	.000
	N	50	50	50	50
Awareness	Pearson Correlation	.770**	1	.726**	.696**
	Sig. (2-tailed)	.000		.000	.000
	N	50	50	50	50
Adoption	Pearson Correlation	.699**	.726**	1	.740**
	Sig. (2-tailed)	.000	.000		.000
	N	50	50	50	50
Blockchain	Pearson Correlation	.725**	.696**	.740**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	50	50	50	50

**. Correlation is significant at the 0.01 level (2-tailed).

The data presented in the table indicate that the observed values of significance are below the threshold of 0.05 ($p = 0.000$). This outcome demonstrates the strong correlation among the inquiries within the diverse constructs of the questionnaire. Therefore, the utilisation of the questionnaire is deemed appropriate for the purpose of gathering primary data in the research study. Therefore, the subsequent section illustrates the methodology employed to collect the data.

3.5 Data Analysis Procedures

Statistical Package for Social Science (SPSS 25) will be utilised for statistical analysis of the data in this research study. In order to ensure that the data was effectively represented, the researcher will be carried out an examination of data entry and missing data, then confirmed that the data is complete before progressing to carry the actual analysis. In addition, the descriptive analysis for each variable will be done to ensure data length is complete for all questions. Following this, the Statistical Package for the Social Sciences (SPSS) was employed to carry out several analytical procedures, including descriptive analysis, factor analysis, reliability analysis, and regression analysis. The utilisation of this particular data analysis approach was chosen due to its distinctiveness in comparison to the methodologies employed in previous research endeavours. The findings of the investigation are displayed through the utilisation of tables, figures, and charts.

3.5.1 Descriptive Analysis

This method of analysis is used to quantitatively describe, examine, or summarise the primary characteristics of obtained data (Coakes and Steed, 2007). Moreover, the process has the capability to transform unprocessed data into more significant insights, hence facilitating the representation of a comprehensive range of aspects inside a given context (Cavana et al., 2001). The present methodology utilises descriptive methods to portray and elucidate a dataset through the use of tables, graphs, and summary measures (Norusis, 2003). The descriptive analysis encompassed many statistical measures, such as standard deviation, mean, minimum, and maximum ranges, in order to assess the final construct (Johnson & Christensen, 2000).

3.5.2 Reliability Analysis

Reliability analysis pertains to the extent to which a measurement scale yields consistent outcomes when the measurements are repeated on multiple occasions (Malhotra, 2007). The determination of reliability analysis involves the acquisition of the fraction of systematic variation present within a given measurement scale. The association between scores received from different scale selections can be determined in order to achieve this. However, in the context of reliability analysis, a high association indicates that the scale consistently produces reliable results. Within this theoretical context, the prevailing indicator of scale reliability is Cronbach's alpha, as established by Field (2005). Cronbach's alpha is a statistical measure used to assess the internal consistency of a set of items or variables. Its values vary from -1.00 to 1.00, with a value of 0 indicating a perfect correlation between two constructs. If the value of alpha exceeds 0.7, it is deemed to be an appropriate measure (Hair et al., 2006).

3.5.3 Spearman Correlation Analysis

This type of analysis is a statistical method used to quantify the degree of relationship between two metric constructs. It typically yields a numerical value ranging from 0 to 1, indicating the level of link between the constructs (Malhotra, 2007). The strength of the relationship between two constructs is directly proportional to the magnitude of the correlation coefficient. The correlation coefficient has the potential to be positive or negative, contingent upon the direction of the association between the two constructs (Hair et al., 2006). Various scholarly sources provide varying interpretations; nevertheless, (Cohen 1988; Pallant 2007) put forth the subsequent guidelines: when the R-value ranges from -0.50 to 1.00, it indicates a strong relationship; when the R-value ranges from -0.30 to 0.49, it indicates an average relationship; and when the R-value ranges from -0.10 to 0.29, it indicates a weak relationship. The following guidelines pertain to the magnitude of the correlation coefficient and its association with the presence of a negative sign in the R-values. The negative sign denotes the direction of the relationship rather than its magnitude. Simultaneously, the measure of strength is denoted by the correlation coefficient, commonly referred to as the R-value. The Spearman correlation coefficient used for this study is a statistical measure that quantifies the degree and direction of the relationship between two or more variables, which are measured on at least one ordinal scale. This metric can be utilised to ascertain the presence or absence of a correlation between the variables. The symbol "rs" is employed to represent this particular notion. The aforementioned test is utilised for variables that are ordinal in nature or for continuous data that do not meet the necessary assumptions for Pearson's correlation.

3.5.4 Ordinal Regression Analysis

The regression analysis is a robust method that offers a versatile approach to examining the associative connections between a metric dependent variable and one or more independent variables (Malhotra, 2007). It is a statistical method employed to investigate and demonstrate the association between different constructs (Hair et al., 2006). The assumption of a linear relationship between the independent and dependent variables is a key principle in regression analysis (Hair et al., 2006). Various forms of regression analysis exist, including simple, hierarchical, and stepwise regression. The selection of a certain kind is contingent upon the variables or constructs under investigation within the study context. The variables included in the regression equation vary according to the respective categories. In accordance with the methodology proposed by Baron and Kenny (1986), an ordinal regression analysis is utilised to investigate the data that does not meet the multiple regression analysis.

The analysis and interpretation of the data would rely on the level of significance ($p > 0.05$), then followed by the Coefficient of determination (R Square) and standardised beta coefficient value for ordinal regression. These measures enable researchers to make direct comparisons about the relative impacts of each independent variable on the dependent variable. Adjusted R-squared values are also provided in this analysis output. Assume that the research endeavour was to examine the impact of incorporating independent factors into the theoretical framework by comparing various combinations of independent variables, varying sample sizes, or both. In this scenario, the adjusted R Square value is appropriate. The coefficient of determination is expected to exhibit an increase as new independent variables are incorporated into the framework. However, it is also possible for the decline to occur if the explanatory power of the newly introduced independent variables is insignificant or if the degree of freedom (df) becomes insufficiently large (Hair et al., 2010).

The discipline of regression analysis encompasses a specialised area referred to as ordinal regression. Ordinal regression is a statistical technique used for predictive analysis, which aims to summarise data and elucidate the association between a dependent variable and two or more independent variables. In the context of conducting an ordinal regression analysis, it is necessary for the dependent variable to possess the characteristic of ordinal data, while the independent variable might be either of continuous or ordinal data type.

3.6 Summary

This chapter carefully and completely clarified the research methodology, data collection strategy and execution, and data analysis, translation, and presentation. The questionnaire instrument for this project is developed and attached to Appendix A of this report document. In the next chapter, data results and analysis are presented to demonstrate respondent contribution towards blockchain usefulness, awareness and adoption toward IoT with developers in Malaysia. This chapter further provides an overview of the methods employed in the research process, as well as the tactics utilised for data gathering. The study's research paradigm, research approach, research design, population, and sample are key components that need to be considered in academic research. This study provides a description of the sample size, data collection method, measurement variables, and data analysis methodologies employed. The researchers regard the population as distinctive on account of the magnitude of the sample. The research design conforms to the principles and procedures of quantitative research methodology. The subsequent chapter presents an analysis of the study's findings.

CHAPTER 4

FINDINGS AND DISCUSSION

4.1 Introduction

This chapter outlines the results from the data analysis and offers an in-depth interpretation of these findings. The chapter plays a vital role as it directly addresses the research objectives and hypotheses presented earlier in the thesis. The data discussed here comes from a survey that was analysed using SPSS version 26. The analysis is crucial for assessing how Blockchain technology is viewed in terms of its perceived usefulness, awareness, and adoption within the IoT sector in Malaysia.

The discussions focus on how the findings align with the research questions and objectives, and how they contribute to a better understanding of Blockchain's role within the IoT ecosystem. This analysis evaluates whether Blockchain is perceived as beneficial, if professionals in the IoT field are aware of its potential, and the level of its implementation in the Malaysian IoT infrastructure. Additionally, the insights presented here inform future studies, policy decisions, and technological strategies within Malaysia's IoT sector. Ultimately, this chapter help determine whether the hypotheses proposed in Chapter 2 are validated by the collected data, furthering the goal of this research to explore the impact of Blockchain technology on Malaysia's IoT ecosystem.

4.2 Response Rate

To achieve the study objectives, a survey was distributed to a sample of 443 respondents, out of which 349 responses were deemed usable for analysis. The sample was selected from a pool of 2,408 ICT/IT companies in Malaysia. Of the 443 returned questionnaires, a 90.5% response rate was achieved, which is considered strong for survey-based research. After excluding incomplete or invalid submissions, 349 usable responses were retained for further analysis, while 94 responses were discarded due to various issues (missing information and inconsistent answers).

Table 4.1 : Respondents Response Rate

Items	Received	Response rate received	Useable	Non-Useable
Frequency	443	90.5%	349	94

These usable responses form the foundation of the analysis, focusing on the adoption of Blockchain in Malaysia's IoT sector. The high response rate highlights the significance of the study to the target audience, thereby strengthening the reliability of the study's conclusions.

4.3 Demographic Profile of the Respondents

The age distribution of respondents highlights some important trends its significance: ***Prevalence of Younger Participants (21–30 years):*** The majority of respondents (likely the largest segment) fall within the 21–30 age range. This suggests that younger professionals are more engaged with Blockchain technology in the IoT ecosystem. Given that this group tends to be more familiar with emerging technologies, they are likely more receptive to adopting Blockchain solutions in IoT applications.

Notable Representation from the 31–40 Years Group: The second-largest group comprises respondents aged 31–40 years. These respondents are generally in the mid-career stage and may have practical experience in IoT development. Their understanding of Blockchain is likely shaped by both technical expertise and the real-world challenges they encounter in the industry. Their perspectives may reflect a blend of theoretical knowledge and hands-on insights.

Lower Representation in Older Age Groups (41–50 and 51–60 years): The smaller proportions of respondents in the 41–50 years (17.77%) and 51–60 years (3.72%) age groups suggest less direct engagement with Blockchain technology in IoT. This could be attributed to generational differences in embracing new technologies. These respondents might have more conventional views on technology integration or may not be as directly involved in the application of advanced technologies like Blockchain in IoT.

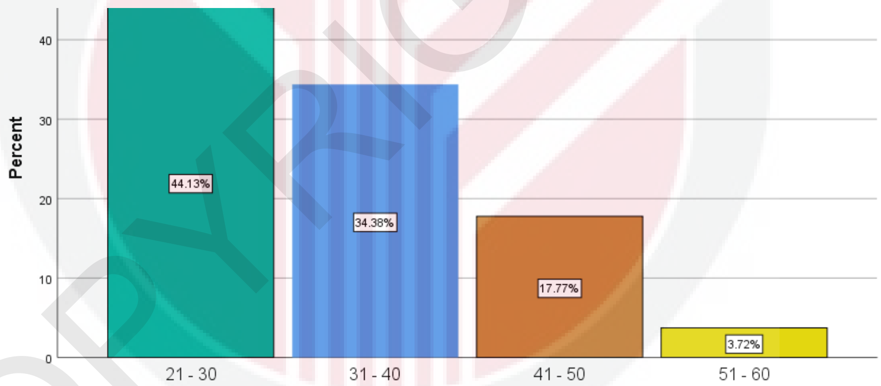

Figure 4.1 : Age Group of the Respondents

Relevance to the Study's Objectives:

Perceived Usefulness: Younger groups may view Blockchain as a highly valuable tool for addressing IoT challenges such as security, data integrity, and scalability. On the other hand, older participants might need more compelling evidence or practical examples to appreciate Blockchain's value in IoT contexts.

Awareness and Understanding: Younger respondents are likely to have greater awareness of Blockchain due to their exposure to digital technologies, which may make them more inclined to adopt such innovations in IoT. In contrast, older participants might require additional resources or education to fully comprehend Blockchain's potential role in the IoT landscape.

Adoption Rate: The age distribution suggests that younger professionals are more likely to drive Blockchain adoption within IoT applications, particularly in roles focused on innovation and development. Adoption may be slower among older groups unless specific educational efforts are introduced to narrow the knowledge gap.

The gender composition of participants is a key demographic factor that can impact the interpretation of the study results concerning Blockchain adoption, awareness, and perceived usefulness within Malaysia's IoT landscape. According to the data, the sample was predominantly male (69.34%), with a smaller proportion of female respondents (30.66%).

Male Predominance: The overrepresentation of male participants (69.34%) is consistent with broader global trends in fields like technology and IoT, where men have traditionally outnumbered women. This can be attributed to several factors, including the higher male participation in STEM (Science, Technology, Engineering, and Mathematics) disciplines and the ongoing gender imbalances in the tech industry. This male-heavy demographic could shape the study's findings, as it may reflect the perspectives and experiences of male professionals, who might have different exposure to or interaction with Blockchain technology compared to women.

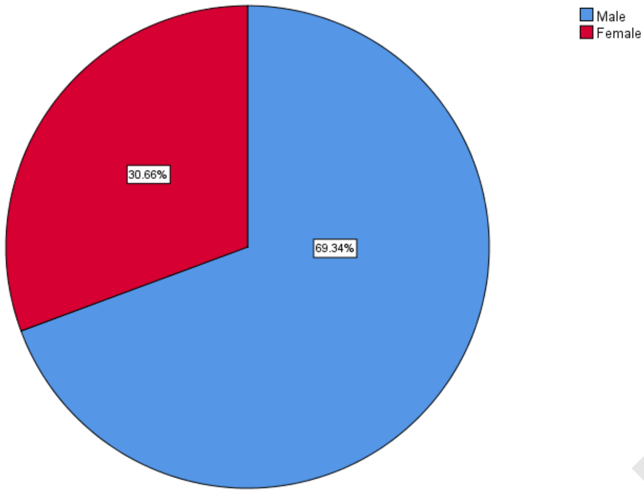

Figure 4.2 : Gender Report of the Respondents

Female Representation: Although the female representation stands at a lower 30.66%, it still comprises a noteworthy portion of the sample. This suggests that there is an increasing presence of women in the IoT and Blockchain sectors, which aligns with efforts to foster more diversity and inclusion in technology fields. The views of female participants may offer valuable insights into the specific challenges or opportunities that Blockchain presents, particularly in terms of its adoption and awareness.

Relevance to the Study's Objectives:

Perceived Usefulness: It is likely that male respondents may report a higher perceived value of Blockchain in IoT applications, reflecting the general trends seen in the tech industry, where men have traditionally dominated tech adoption. On the other hand, female respondents could offer a different outlook on how Blockchain could impact IoT, contributing to a more diverse understanding of its potential benefits.

Awareness and Understanding: The larger male respondent group may indicate that the findings related to Blockchain awareness and understanding are predominantly shaped by male viewpoints. However, the smaller female sample could provide important perspectives on how women in tech engage with Blockchain technology, including any unique obstacles they face in understanding or adopting it within the IoT context.

Adoption Rate: The gender breakdown might also influence adoption trends. With more male respondents, it is possible that Blockchain adoption trends may be somewhat biased towards male-driven initiatives. However, insights from female participants could shed light on specific barriers women may encounter in adopting Blockchain solutions for IoT development.

The data on workforce distribution, gathered from the research questionnaire, offers key insights into the organizational roles of the participants. This is crucial for understanding how individuals across different levels of responsibility perceive and interact with Blockchain technology within Malaysia's IoT ecosystem.

Lower Employee Level (61.89%): The majority of respondents (61.89%) belong to lower employee levels, indicating that most respondents are engaged in operational and technical tasks. This group likely includes IoT developers, engineers, and technicians who are directly involved in the implementation of Blockchain technology in IoT applications. Their perspectives are important for understanding the practical challenges of using Blockchain, as well as how it is perceived at the operational level, especially in terms of day-to-day implementation.

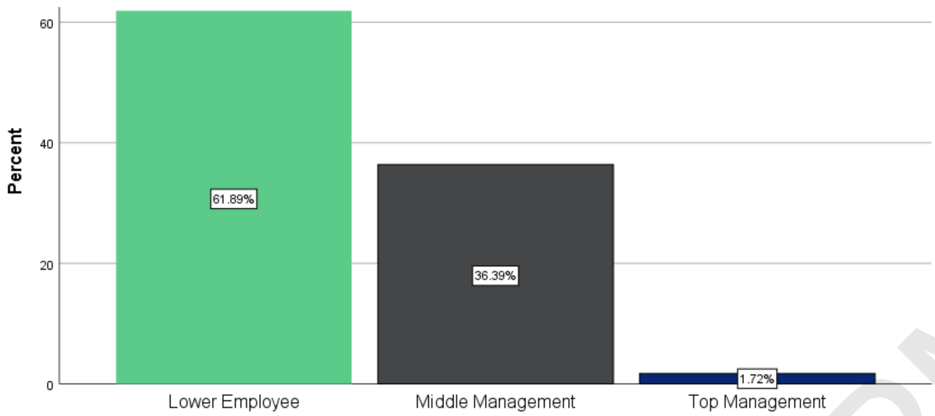

Figure 4.3 : Workforce Position Report of the Respondents

Middle Management (36.39%): A significant portion of respondents (36.39%) are from middle management. These individuals act as a bridge between senior leadership and lower-level employees. Middle managers are likely to have a broader understanding of Blockchain's potential within IoT, including its impact on efficiency, security, and scalability. Their role in decision-making processes concerning technology adoption also gives them valuable insights into the organization's readiness to embrace Blockchain.

Top Management (1.72%): The smallest group of respondents (1.72%) comes from top management. Despite their limited representation, their input is still critical in understanding the strategic approach to adopting Blockchain technology. Senior leaders typically assess technological innovations with a focus on long-term business objectives and maintaining a competitive edge. The small proportion of responses from top management could indicate that the decision to adopt Blockchain is often led by middle management, with senior leadership offering overall direction.

Relevance to the Study's Objective:

Perceived Usefulness: Lower-level employees might view Blockchain primarily in terms of its impact on their daily work tasks, such as ensuring data integrity and automating processes. Middle management, with a more strategic outlook, may focus on the technology's potential to optimize processes, enhance security, and improve scalability within IoT solutions. The small number of responses from top management suggests that they may perceive Blockchain's value more in terms of aligning with organizational goals and long-term vision, rather than its immediate practical applications.

Awareness and Understanding: The large representation of lower-level employees suggests that their awareness and understanding of Blockchain are shaped by its direct application and the challenges they encounter. Middle management, on the other hand, may have a more comprehensive view, understanding Blockchain's broader strategic implications for the organization. The low involvement of top management in the survey point to their focus on other high-priority areas, despite being aware of Blockchain's strategic value.

Adoption Rate: The larger share of responses from lower and middle management suggests that their perspectives are more grounded in the actual challenges and opportunities related to Blockchain adoption. These groups play a crucial role in the practical integration of Blockchain into IoT solutions. In contrast, top management's involvement seems to focus more on approving the adoption process and allocating resources, while middle management is likely to drive the technology's implementation.

The diverse educational backgrounds of the respondents offer a range of perspectives, from theoretical and strategic insights (from PhD and master’s degree holders) to more practical, hands-on views (from bachelor’s, diploma holders, and those without formal higher education). Recognizing these variations is essential for understanding how Blockchain is viewed and its potential adoption within Malaysia’s IoT sector. The differences in educational levels highlight the varying degrees of technical knowledge and real-world experience among the respondents, which influence how Blockchain is perceived and integrated across different sectors of the workforce

A significant majority (89.11%) of respondents have completed higher education, suggesting they possess a strong foundation in technical subjects, which is crucial when assessing advanced technologies such as Blockchain in the IoT sector. This indicates that the participants likely have a good grasp of technological concepts, allowing them to engage with the technical, practical, and strategic aspects of Blockchain implementation.

PhD Holders (14.04%): About 14.04% of respondents hold a PhD, indicating they possess deep technical knowledge and a thorough understanding of the theoretical principles behind technologies like Blockchain. These individuals are expected to offer a more in-depth, research-oriented perspective on Blockchain’s potential, focusing on areas like scalability, security, and its theoretical advantages compared to traditional technologies.

Master’s Degree Holders (26.07%): A quarter of the respondents (26.07%) have earned a master's degree, indicating they likely specialize in technology or fields related to IoT. This group is well-positioned to understand both the theoretical and practical aspects of Blockchain technology. They can offer valuable insights into how Blockchain can be applied to real-world IoT solutions, addressing both its opportunities and challenges.

Bachelor's Degree Holders (28.08%): The largest group (28.08%) holds a bachelor's degree, suggesting they possess fundamental knowledge in technical or engineering disciplines, which is essential for understanding how Blockchain can integrate with IoT systems. Their views are likely more focused on the practical applications of Blockchain, especially in terms of solving specific technical issues within the IoT environment.

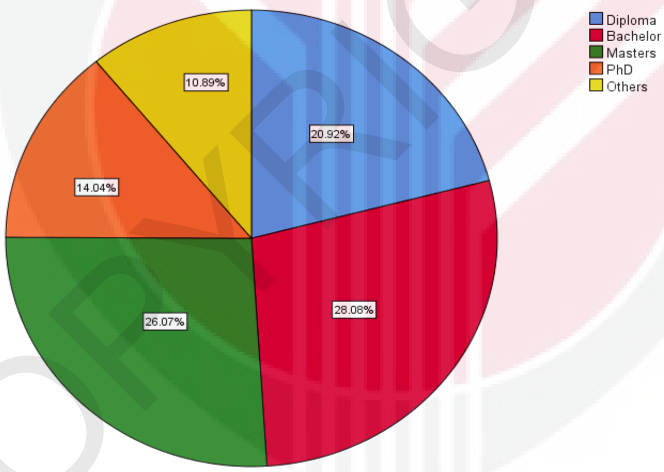

Figure 4.4 : Education Level Report of the Respondents

Diploma Holders (20.92%): A smaller segment (20.92%) holds a diploma, typically reflecting more vocational or technical training. Although they may not have the same depth of theoretical knowledge, this group brings hands-on experience and could offer valuable insights into how Blockchain can be applied to solve practical challenges in IoT operations.

Respondents Without Higher Education (10.89%): A small portion of respondents (10.89%) lack formal higher education. While their theoretical knowledge of technologies like Blockchain might be limited, they could still provide meaningful insights based on practical experience with IoT systems, shedding light on real-world challenges and opportunities.

Relevance to the study's objective:

Perceived Usefulness: The perception of Blockchain's effectiveness may vary based on education levels. PhD and master's degree holders are expected to see Blockchain as a robust, scalable solution with far-reaching potential. Conversely, those with diplomas or less formal education might view it primarily as a tool for addressing practical issues in IoT, such as improving security or streamlining processes.

Awareness and Understanding: Given the high number of respondents with advanced degrees (PhD, master's, and bachelor's), it is likely that most participants possess a solid understanding of Blockchain technology. They are more likely to appreciate its potential within IoT systems and recognize the challenges it might present. However, those with lower levels of education, such as diploma holders or those without formal education, may have a more hands-on or operational understanding, with limited exposure to Blockchain's theoretical aspects.

Adoption Rate: Educational background may also influence the likelihood of Blockchain adoption. Those with advanced degrees might be more inclined to endorse and adopt Blockchain in IoT applications, as they are more familiar with its strategic and technological benefits. On the other hand, respondents with lower levels of education may encounter obstacles in adopting these new technologies unless they receive practical demonstrations or targeted training.

The data on respondents' work tenure offers crucial insight into their experience levels within their respective sectors, which is essential for understanding their views on the adoption, usefulness, and awareness of Blockchain technology in Malaysia's IoT ecosystem. The variation in tenure provides a deeper understanding of how experience might shape attitudes toward emerging technologies like Blockchain.

Under 5 Years (45.27%): Almost half of the respondents (45.27%) have less than five years of experience in their respective fields. This group likely includes individuals who are relatively new to their industries, and their understanding of IoT and Blockchain is probably influenced by recent educational experiences and exposure to the latest technological trends. These respondents might be more inclined to embrace innovations such as Blockchain and more open to its integration within IoT systems, especially if their education reflects current technological advancements.

5 to 10 Years (32.66%): The next largest group (32.66%) has between 5 to 10 years of experience. These respondents likely have a firm grasp on both conventional and emerging technologies, with their perspectives on Blockchain shaped by hands-on industry experience and the evolution of IoT in recent years. They may offer insights into the practical implications, challenges, and opportunities for adopting Blockchain in IoT applications.

11 to 15 Years (12.32%): A smaller segment of respondents (12.32%) has between 11 and 15 years of experience. This group is probably well-versed in industry-specific practices, but their longer tenure might lead them to adopt a more cautious stance toward new technologies like Blockchain. They could be more hesitant to implement such innovations unless they are convinced of their proven effectiveness.

16 to 20 Years (6.59%): Only 6.59% of respondents have 16 to 20 years of experience. These respondents likely have substantial expertise in their fields and may be more resistant to adopting new technologies like Blockchain unless clear evidence supports its long-term benefits. While they may prioritize stability and proven solutions, they can provide valuable perspectives on how Blockchain could potentially disrupt and enhance traditional practices.

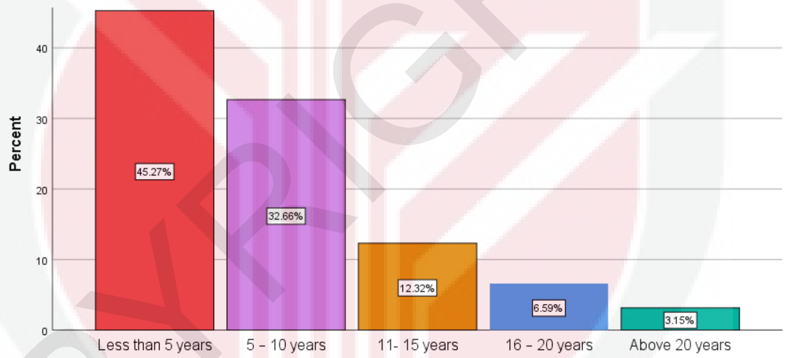

Figure 4.5 : Respondents Work Tenure

Over 20 Years (3.15%): A small proportion (3.15%) of respondents has over 20 years of industry experience. This group brings extensive knowledge and could offer a historical view on the development of IoT and Blockchain. Though they may have a more conservative approach to technology adoption, their input could be pivotal in understanding how Blockchain might reshape established systems and its future role in IoT.

Relevance to the Study's Objective:

Perceived Usefulness: The perceived value of Blockchain in IoT applications might differ according to work tenure. Professionals with shorter tenures might view Blockchain as an essential and innovative solution, while those with more experience may require stronger evidence of its potential impact on current challenges in IoT.

Awareness and Understanding: Those with shorter tenures (less than 5 years) may be more familiar with recent advancements in Blockchain and IoT, suggesting a higher awareness and enthusiasm for emerging technologies. In contrast, professionals with longer careers (more than 10 years) may hold more traditional views, which could result in lower awareness or skepticism toward new technologies like Blockchain.

Adoption Rate: The adoption of Blockchain technology is likely to be led by respondents with shorter tenures who are more receptive to new technologies. Mid-tenure professionals (5-10 years) may be instrumental in navigating the balance between adopting Blockchain and managing its practical integration. Meanwhile, those with longer tenures may be slower to adopt unless the benefits are clearly demonstrated.

The breakdown of respondents by industry also offers valuable insight into the variety of sectors engaged in the study and sheds light on how Blockchain technology is understood, embraced, and utilized across different industries within Malaysia's IoT ecosystem. The varying participation levels from different sectors also help to identify which industries are most actively exploring the intersection of Blockchain and IoT, while also revealing where gaps in knowledge or adoption might exist.

Cloud Hosting, Online Services & Retail (26.9%): The Cloud Hosting, Online Services & Retail sector, contributing 26.9% of respondents, represents the highest level of engagement. This sector is inherently tied to digital innovation, with a focus on data management, security, and service delivery—areas where Blockchain can play a transformative role. The strong response rate suggests that professionals in these fields are likely well-versed in Blockchain's potential, particularly in enhancing data integrity, securing transactions, and improving operational efficiencies within IoT frameworks.

Data Mining (24.1%): Data Mining, with 24.1% of responses, follows closely behind. Given its data-centric nature, this sector stands to benefit significantly from Blockchain's ability to ensure the security, authenticity, and transparency of data. Respondents from this industry are likely interested in Blockchain's application in tackling challenges like data provenance, audit trails, and decentralized data management, especially within IoT systems.

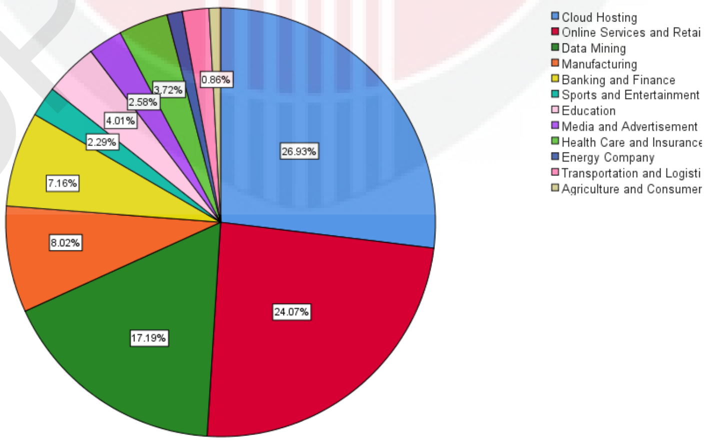

Figure 4.6 : Respondents Work Sectors

Manufacturing (17.2%): The Manufacturing sector's 17.2% response rate reflects its growing interest in Blockchain for use cases such as optimizing supply chains, improving traceability, and securing IoT-connected devices. Participants from this industry likely see Blockchain as a means to solve operational inefficiencies and address security vulnerabilities, helping to streamline production processes within IoT-enabled systems.

Banking and Finance (7.2%): Banking and Finance accounted for a smaller proportion of responses (7.2%). Despite Blockchain's potential to revolutionize transaction security, reduce fraud, and improve financial services, this sector's relatively low response rate may suggest a focus on traditional financial models rather than exploring emerging technologies like IoT. However, as Blockchain continues to evolve, its relevance in the financial sector is expected to grow.

Other Sectors (Sports, Entertainment, Education, Media, and Advertising): Sectors such as Sports and Entertainment (2.3%), Education (4.0%), and Media and Advertising (2.6%) made up a smaller share of responses. While Blockchain may not be at the forefront in these industries when it comes to IoT applications, niche use cases such as secure ticketing, media rights management, and credential verification could still be areas of interest for Blockchain adoption.

Healthcare and Insurance, Energy, Transportation, Agriculture, and Consumer Commerce: Healthcare and Insurance (3.7%), Energy (1.1%), Transportation and Logistics (2.0%), and Agricultural and Consumer Commerce (0.9%) sectors had lower response rates. These industries may be slower to adopt Blockchain, possibly due to their more traditional infrastructures. Nevertheless, emerging applications like patient data management in healthcare or supply chain transparency in energy could increase Blockchain's relevance in these fields in the near future.

Relevance to the Study's Objective:

Perceived Usefulness: In industries like cloud hosting, online services, and data mining, Blockchain is likely seen as a highly valuable technology to enhance security, transparency, and scalability within IoT ecosystems. Manufacturing may also perceive Blockchain as a key solution for improving supply chain management and production efficiency. Although banking and finance have been slower to adopt Blockchain in the IoT context, they still recognize its potential for enhancing transaction systems and reducing fraud.

Awareness and Understanding: Sectors with higher response rates, such as cloud hosting, online services, retail, and data mining, are more likely to have a deeper understanding of Blockchain and its potential in IoT applications. These industries are already involved in digital transformation and may have a higher level of familiarity with Blockchain's capabilities. Conversely, sectors like agriculture and transportation may exhibit less awareness due to their more traditional operational models.

Adoption Rate: Blockchain adoption is expected to be more widespread in sectors with a higher representation in the study, such as cloud hosting, online services, and data mining, as these industries are more proactive in integrating emerging technologies. On the other hand, sectors like healthcare, energy, and agriculture, with fewer respondents, may be in earlier stages of exploring Blockchain, or may require more compelling use cases to drive adoption.

The information about the size of the organizations where the participants are employed offers valuable context for interpreting their views on Blockchain technology in the IoT ecosystem. The scale of the firms they work for, along with their operational capabilities, can shape how Blockchain is perceived, implemented, and integrated into business practices.

Small Firms (71.6%): A large portion (71.6%) of the respondents work in small firms. These organizations typically have fewer resources and may specialize in niche areas. Their interest in Blockchain could stem from its potential to reduce costs, enhance data security, or boost efficiency through automation. Due to their flexible structure, small businesses may be more open to adopting new technologies like Blockchain. However, challenges such as limited technical expertise or restricted budgets for large-scale implementation may arise.

Medium-Sized Enterprises (18.6%): A smaller proportion (18.6%) of participants are employed by medium-sized enterprises. These businesses generally have more resources than small firms and may already be incorporating advanced technologies. Their adoption of Blockchain could be viewed as a strategic move to scale operations, strengthen security, or optimize supply chain management. For medium-sized enterprises, Blockchain could be part of a wider digital transformation plan, particularly in industries like IoT where data management and security are vital.

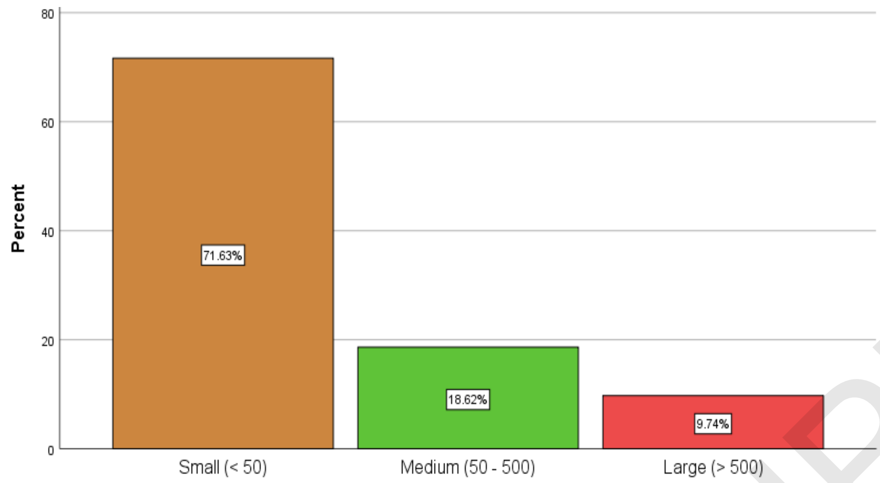

Figure 4.7 : Respondents Firm Size

Large Enterprises (9.7%): Only a small percentage (9.7%) of respondents work for large enterprises. These organizations usually have established infrastructures and may engage in long-term investments in technologies like Blockchain to improve security, compliance, and scalability within IoT systems. However, their larger size often means more complex decision-making processes, and the implementation of Blockchain on a large scale can be more challenging. While large enterprises could lead Blockchain adoption in certain sectors, they might approach it more cautiously and methodically compared to smaller businesses.

Relevance to the Study's Objective:

Perceived Usefulness: The perceived value of Blockchain is likely to vary with company size. In small firms, the focus might be on immediate, practical benefits, such as cost savings, data integrity, and secure transactions. In medium enterprises, Blockchain could be seen as a scalable solution to enhance operational efficiency, security, and supply chain management. For large enterprises, Blockchain's value might be primarily associated with its capacity to manage large volumes of data and transactions securely while meeting regulatory requirements.

Awareness and Understanding: The size of the company can significantly influence the depth of knowledge and awareness of Blockchain technology. Employees in small firms might have a more hands-on, practical approach to Blockchain, focusing on how it can streamline operations and enhance efficiency in specific tasks. Those in medium-sized enterprises may take a more strategic view, understanding both the operational and broader organizational benefits. Employees of large enterprises might have a more formalized and comprehensive understanding of Blockchain, particularly in terms of scalability, security, and regulatory compliance.

Adoption Rate: Blockchain adoption is likely to be more prevalent in medium and large enterprises, where more resources are available for technological initiatives. Small firms, while more adaptable, may adopt Blockchain more cautiously, seeking clear, cost-effective benefits before committing. Nevertheless, smaller firms could still play a key role in early-stage adoption and experimentation, especially in industries that prioritize innovation and agility.

The distribution of respondents across different firm sizes offers essential context for understanding the study's results. With the majority employed in small firms, their perspectives are likely cantered around the practical, cost-effective applications of Blockchain. On the other hand, medium and large enterprises are likely to have a more strategic, long-term outlook on Blockchain's potential, particularly with respect to scalability, security, and compliance. These differences are crucial for evaluating how Blockchain is perceived, understood, and adopted in the context of Malaysia's IoT ecosystem. The breakdown of firm sizes is instrumental in analysing varying levels of awareness and adoption trends for Blockchain technology across different firms.

Table 4.2 : Demographic Data Summary

Particulars	Category	Frequency	Percent
Age	21 - 30	154	44.1
	31 - 40	120	34.4
	41 - 50	62	17.8
	51 - 60	13	3.7
	Total	349	100.0
Gender	Male	242	69.3
	Female	107	30.7
	Total	349	100.0
Work Position	Lower Employee	216	61.9
	Middle Management	127	36.4
	Top Management	6	1.7
	Total	349	100.0
Education Level	Diploma	73	20.9
	Bachelor	98	28.1
	Masters	91	26.1
	PhD	49	14.0
	Others	38	10.9
	Total	349	100.0
Work Tenure	Less than 5 years	158	45.3
	5 – 10 years	114	32.7
	11- 15 years	43	12.3
	16 – 20 years	23	6.6
	Above 20 years	11	3.2
	Total	349	100.0
Firm Sectors	Cloud Hosting	94	26.9
	Online Services and Retails	84	24.1
	Data Mining	60	17.2
	Manufacturing	28	8.0
	Banking and Finance	25	7.2
	Sports and Entertainment	8	2.3
	Education	14	4.0
	Media and Advertisement	9	2.6
	Health Care and Insurance	13	3.7
	Energy Company	4	1.1
	Transportation and Logistics	7	2.0
	Agriculture and Consumer Trade	3	.9
	Total	349	100.0
Enterprise Size	Small (< 50)	250	71.6
	Medium (50 - 500)	65	18.6
	Large (> 500)	34	9.7
	Total	349	100.0

4.4 Descriptive Statistics

The statistical data presented in the table 4.3 supports the study’s objectives by offering valuable insights into the perceived usefulness, awareness, and adoption of Blockchain technology within Malaysia's IoT sector. Concerning ***perceived usefulness (Objective 1)***, the data shows generally favourable views, with mean scores ranging from 3.19 to 3.62. The highest mean (3.62) is found in Usefulness 2, accompanied by low variability, suggesting a broad consensus among respondents that Blockchain holds significant value for IoT applications. ***For awareness and understanding (Objective 2)***, the Awareness category indicates an increasing recognition of Blockchain technology among IoT developers, with mean scores between 3.20 and 3.50. The highest mean score (3.50) is seen in Awareness 4, signalling a promising level of awareness. However, moderate variability in the responses suggests that there are still some disparities in the depth of understanding across the respondents.

Table 4.3 : Summary of the Inherent Data Descriptive Statistics

	N	Minimum	Maximum	Sum	Mean	Std. Deviation	Variance
Usefulness1	349	1	5	1192	3.42	1.166	1.358
Usefulness2	349	1	5	1265	3.62	1.162	1.350
Usefulness3	349	1	5	1115	3.19	1.046	1.094
Usefulness4	349	1	5	1192	3.42	1.146	1.313
Usefulness5	349	1	5	1178	3.38	1.157	1.339
Awareness1	349	1	5	1177	3.37	1.111	1.234
Awareness2	349	1	5	1204	3.45	1.168	1.363
Awareness3	349	1	5	1208	3.46	1.125	1.266
Awareness4	349	1	5	1222	3.50	1.181	1.394
Awareness5	349	1	5	1117	3.20	1.064	1.132
Adoption 1	349	1	5	1131	3.24	1.116	1.247
Adoption 2	349	1	5	1139	3.26	1.129	1.275
Adoption 3	349	1	5	1137	3.26	1.180	1.393
Adoption 4	349	1	5	1130	3.24	1.111	1.234
Adoption 5	349	1	5	1111	3.18	1.130	1.277
BIoT 1	349	1	5	1216	3.48	1.467	2.153
BIoT 2	349	1	5	1211	3.47	1.370	1.876
BIoT 3	349	1	5	1247	3.57	1.301	1.694
BIoT 4	349	1	5	1155	3.31	1.403	1.967
BIoT 5	349	1	5	1135	3.25	1.341	1.798
Valid N (listwise)	349						

In terms of ***adoption rate (Objective 3)***, the Adoption category shows mean scores between 3.18 and 3.26, indicating a moderate level of adoption. While these scores are somewhat lower than those for perceived usefulness and awareness, they suggest that although IoT developers recognize the potential of Blockchain, actual implementation is progressing more slowly. The findings highlight generally positive views of Blockchain's usefulness, an upward trend in awareness, and moderate adoption levels. These results point to ongoing progress in integrating Blockchain into Malaysia's IoT ecosystem, though further efforts are needed to accelerate its adoption.

4.5 Constructs' Reliability

The utilisation of reliability analysis is employed to determine the extent of internal consistency in the study's inherent data measurement. Field (2005) found that the researcher's conclusion was that the dependability levels of all variables were deemed satisfactory, as they surpassed the criterion of 0.70. The dependability alpha coefficient values of the four variables are presented in Table 4.9. The variable with the highest coefficient is adoptability rate of Blockchain, with a value of 0.917, this is followed by the IoT ecosystem at 0.913. The usefulness and awareness of Blockchain has a coefficient of 0.887 and 0.891 respectively. Each construct demonstrates a high level of reliability, and all necessary criteria have been fulfilled.

Table 4.4 : Constructs' Reliability Analysis

Name of Variables	No. of Items	Cronbach's Alpha
Usefulness	5	0.887
Awareness	5	0.891
Adoption	5	0.917
Blockchain IoT	5	0.913

4.6 Spearman Correlation Analysis

On the Spearman's correlation test employed to assess the association between each independent variable and the dependent variable. The significance of the correlation coefficient is established when the p-value derived from the statistical analysis is below the threshold of 0.05. According to the findings presented in Table 4.5, it can be observed that both independent factors have a positive impact on the IoT ecosystem. There is no issue of multicollinearity among the variables as their correlation coefficients, denoted as r values, are all below 0.5.

Table 4.5 : Spearman's rho Correlation Analysis

			Usefulness	Awareness	Adoption	Blockchain
Spearman's rho	Usefulness	Correlation Coefficient	1.000	.498**	.545**	.486**
		Sig. (2-tailed)	.	.000	.000	.000
		N	349	349	349	349
	Awareness	Correlation Coefficient	.498**	1.000	.571**	.467**
		Sig. (2-tailed)	.000	.	.000	.000
		N	349	349	349	349
	Adoption	Correlation Coefficient	.545**	.571**	1.000	.528**
		Sig. (2-tailed)	.000	.000	.	.000
		N	349	349	349	349
	Blockchain	Correlation Coefficient	.486**	.467**	.528**	1.000
		Sig. (2-tailed)	.000	.000	.000	.
		N	349	349	349	349

**. Correlation is significant at the 0.01 level (2-tailed).

According to Guilford's (1965) research, a range of r-values between 0.41 to 0.70 indicates a favourable connection. The variable of adoptability (0.528) demonstrates a more robust correlation with the IoT ecosystem, whereas usefulness (0.486), and awareness (0.467) follows suit of a favourable connection with the IoT ecosystem. Therefore, it may be concluded that both independent variables had a favourable correlation with the IoT ecosystem. The researchers ran a Spearman's correlation test using the dependent variable (IoT ecosystem) in order to assess the statistical significance of the independent variables and their influence on the dependent variable. The study necessitated the inclusion of components with a P value ranging from 0.00 to 0.05 in order to establish statistical significance. Table 4.5 presents the results indicating a substantial correlation between independent and dependent success, as evidenced by a p-value of 0.000, which is below the conventional threshold of 0.05, hence verifying the statistical significance of the observed association. The relationship between the independent and dependent variable has shown a substantial association, as evidenced by the p-value of 0.000.

4.7 Ordinal Regression Analysis

Ordinal regression analysis is utilised to investigate the association between independent variables, namely usefulness, awareness, and adoptability rate of Blockchain, and dependent variables, specifically IoT ecosystem. The analysis was conducted by the researcher in order to examine and evaluate the validity of the three hypotheses that were put forth. The findings are displayed in tables 4.6, 4.7, and 4.8.

Table 4.6 : Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	529.021			
Final	303.489	225.532	12	.000

Link function: Logit.

The -2 log-likelihood values for both the intercept model and the entire model, which includes the complete prediction set, are provided in Table 4.6. Therefore, a chi-square probability ratio test was conducted to ascertain if the model of fit of the final model is significantly better than that of the intercept model. In this specific case, it has been established that there exists a statistically significant distinction between the adequacy of the ultimate model and the intercept model. The results revealed a significant chi-square statistic, χ^2 (4) = 225.532, $p < 0.000$, indicating that the independent variables usefulness, awareness, and adoptability rate substantially enhance the model's predictive capability for the IoT ecosystem. This outcome highlights the goodness of fit of the model, confirming that these independent variables are critical in explaining the variability within the IoT ecosystem and aligning the model predictions closely with the observed data.

Furthermore, the outcome obtained is regarded as an approximation representation of the R-squared metric employed in ordinal regression, which corresponds to the pseudo-R-squared values displayed in Table 4.7. The existing body of literature lacks definitive guidance on the practical use and interpretation of this finding (Pituch and Stevens, 2016). However, Petrucci (2009) provides an elucidation of the R-squared measure, wherein the "Nagelkerke" coefficient elucidates a specific proportion of the variance in the dependent variable by considering a specific proportion of the variance in the independent variable (namely, usefulness, awareness, and adoptability rate of Blockchain).

Table 4.7 : Pseudo R-Square

Cox and Snell	.476
Nagelkerke	.500
McFadden	.214

Link function: Logit.

The Nagelkerke statistic value obtained in this study is 0.500, suggesting that the independent factors, namely usefulness, awareness, and adoptability rate of Blockchain, account for approximately 50% of the variability observed in the dependent variable, which is the IoT ecosystem. In addition to the pseudo-R-squared result, Osborne (2017), explains ordinal regression to be predicated on the premise that the connection between the independent variables remains consistent throughout all comparing alternatives encompassing the dependent variables. If the results of the parallel line test indicate a lack of significance, it can be decided that the condition has been met.

Table 4.8 : Test of Parallel Lines

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Null Hypothesis	303.489			
General	267.650[b]	35.839[c]	36	.476

The lack of statistical significance is commonly taken as supporting evidence for the validation of the hypothesis. Based on the analysis of this study, as indicated in Table 4.8, the outcome is deemed to support the hypothesis due to the fact that its p-value exceeds the threshold of .005. The test findings utilising parallel lines indicate that the previously established correlation between each variable remains accurate. The findings indicate that there is a substantial relationship between all the factors and IoT ecosystem success, as evidenced by their p-values over 0.05. Consequently, the null hypotheses are refuted, while the alternative hypotheses are upheld. Moreover, it can be argued that the implementation of Blockchain technology has a substantial impact on the IoT ecosystem.

4.8 Discussion of Findings and Results

The examination and analysis of the outcomes and discoveries derived from the investigation have contributed to the expansion of the existing body of literature and understanding within the realm of blockchain with IoT ecosystem industries, as well as among scholars engaged in research in this field. Hence, the analysis of the results will be emphasised in relation to the research inquiries posited in the investigation.

4.8.1 What Role Does Blockchain Play in the IoT

This section examines the significant contributions of blockchain technology in enhancing the realm of IoT applications. These contributions encompass the provision of robust scalability, the preservation of comprehensive data privacy, and the facilitation of interoperability and orchestration among connected devices. In the context of IoT environments, a substantial influx of devices occurs, leading to a notable decrease in network performance and a significant increase in associated expenses. The reason for this delay is the need to verify and authenticate a vast number of microtransactions taking place across interconnected devices. The absence of scalability results in significant delays in the process of verifying transactions. The blockchain technology incorporates a rapid consensus mechanism to facilitate enhanced scalability (Wen et al., 2020; Perez et al., 2020).

The finding of this study is consistent with Veena (2015), where the shift from a centralised network to a peer-to-peer distributed network is expected to mitigate the occurrence of central failures and constraints. Additionally, it is beneficial to prevent situations in which a few numbers of corporate entities control the management and retention of vast amounts of individuals' data. Additional role of decentralising the IoT encompasses enhanced system scalability and heightened fault tolerance. Hence, the statistical analysis revealed that the usefulness of Blockchain implementation had a considerable impact on the IoT ecosystem in Malaysia. Thus, it may be concluded that hypothesis H_1 received significant and favourable support.

Employing blockchain into the IoT ecosystem will facilitate the coordination of IoT infrastructure and smart contracts within a specified context. Smart contracts play a crucial role in determining the decision-making processes within blockchain networks that are pertinent to IoT devices. The utilisation of blockchain technology enables the effective coordination of many IoT operations. These operations encompass the administration of access to and from smart devices, the advancement and processing of data, the dynamic location of devices, and the modification of containers, such as software devices (Lee and Park, 2021). The coordination of IoT device operations is linked to various trust and security considerations. These include the need to document the identities of all IoT entities within the system, track the origins of device data and other entities that enter the IoT system, and record the processing procedures through the utilisation of smart contracts (Shbair, 2018).

4.8.2 How is the Awareness Level of Blockchain to IoT Developers

The utilisation of blockchain technology and cryptocurrencies has already exerted a significant influence on both individuals and enterprises within the context of Malaysia (Ku Ruhana et al., 2019). Participation in this endeavour is not contingent upon one's educational attainment, age, or specific industry affiliation. As of 2017, the understanding of blockchain and its associated technologies has reached an intermediate level, with a limited number of individuals considered experts in the field (Anthony et al., 2018). The current blockchain community in Malaysia employs the technology in diverse manners, including its utilisation for Peer-to-Peer payment systems. In addition to Bitcoin, the blockchain community possesses knowledge of Ethereum. A significant number of individuals have acquired multiple types of cryptocurrencies, primarily motivated by financial purposes. Their participation is driven by a strong belief in the tokens' long-term vision and worth (Zulhuda & Sayuti, 2017). However, the advancement of technologies may face obstacles due to governmental control. Currently, the Central Bank of Malaysia has yet to provide any official guidelines pertaining to blockchain adoption in the FinTech Industry. This research further prioritises the investigation of awareness among communities in Malaysia that are not specifically focused on blockchain, as well as the development of applications utilising blockchain technology.

The primary purpose of awareness both in IoT and blockchain was not to establish mutual discovery as the concept of blockchain was not initially designed for the IoT (Farahani et al, 2021). The successful integration of blockchain to the IoT ecosystem is contingent upon the extent of knowledge and awareness around both blockchain and IoT technologies. Unfortunately, in many disciplines, this level of understanding remains rather low as shown in this study finding correlation coefficient of 0.467. This knowledge gap is exacerbated by the growing disparity between the information possessed by individuals in various domains and the rapidly advancing industrial technology (Rifi et al., 2017). Moreover, there is a significant dearth of resources that offer a comprehensive overview of emerging technologies such as cloud computing, the IoT, security measures, encryption techniques, and blockchain.

In order to facilitate the integration of blockchain technology inside the IoT ecosystem sector, a fundamental shift in cultural norms and practices is necessary. The prevailing IoT ecosystem predominantly exhibits a centralised and manual structure, rendering them susceptible to data breaches and single points of failure. However, it is important to note that in the current context of blockchain technology, there is a lack of persons who possess the necessary level of education and skills to effectively oversee complex peer-to-peer networks (Mettler, 2016; Simić et al, 2017). The demand for work associated with blockchain technology has shown a significant increase of approximately 2000% during recent years. However, the challenge of locating proficient programmers has emerged as a significant concern. Due to the nascent stage of blockchain technology, it is expected that the Malaysia IoT development community would require a considerable amount of time to fully adopt and integrate blockchain (Yaqoob et al., 2021). Hence, hypothesis H_2 was significantly supported.

4.8.3 What is the Adoptability Rate of Blockchain with IoT

According to recent data in developed nations, a significant proportion, specifically 75%, of individuals or organisations in the developed nations have embraced IoT technology with included blockchain technology into their operations or have intentions to do so by the conclusion of the year 2030. Within the community of organisations that have embraced blockchain technology, a significant majority of 86% have chosen to integrate this technology with other complementary technologies in diverse initiatives. The obtained results exhibit a high level of significance and beyond initial expectations in terms of strength. Despite the nascent stages of acceptance for both blockchain and IoT technologies, organisations have begun integrating them to achieve positive business outcomes (Costello, 2019).

IoT companies are increasingly recognizing the crucial necessity of incorporating Blockchain technology into their operations as a result of its extensive range of opportunities for innovation and distinctiveness. The utilisation of Blockchain technology enables developers to construct decentralised applications without the need for centralised server communication. Consequently, IoT developers are now equipped with options of producing reliable applications that are subject to thorough examination (Ali et al., 2018). Smart contracts, referred to as SCs, are programmable agreements that may be included into the Blockchain-IoT infrastructure, enabling them to operate autonomously. As a result of this phenomenon, numerous organisational protocols have the potential to be optimised and mechanised, hence eliminating intermediaries and yielding cost savings (Jackson et al., 2024). Furthermore, the adoption of Blockchain technology into IoT has the potential to augment the levels of data security, privacy, and management, which are fundamental elements within the realm of contemporary IoT engineering (Vizcaino Naranjo et al., 2023). The implementation of blockchain technology has the potential to enhance the productivity, safety, and market access of IoT enterprises.

Some developers and organisations within the industry are presently engaged in the development of use cases that integrate both technologies, as their combined utilisation presents a viable means of mitigating security vulnerabilities and associated business hazards. The level of blockchain adoption has a notable impact on the readiness of developers to adopt blockchain technology into the IoT ecosystem. The concept of adoption is widely recognized as a crucial factor in promoting the preparedness of developers to adopt new technology into their existing architecture. The study revealed that the coefficient between blockchain adoption readiness and IoT ecosystem was estimated to be 0.528, indicating a statistically significant relationship with a p-value of less than 0.005. These values supported the third hypothesis. The results of the study suggest that within the context of organisational preparedness, the level of adoption exhibited by decision makers in the IoT sector has a significant role in determining the readiness of organisations to embrace Blockchain technology into the sector. Therefore, the findings presented in this study are in alignment with the outcomes reported in prior research studies (Ullah et al., 2020; Razali et al., 2023). The research findings indicate that adoption is a characteristic that not only inclines individuals to engage in experimentation with novel technological advancements but also has a favourable impact on their willingness to accept such innovations (Nuryyev et al., 2021). Hence, hypothesis H_3 was significantly supported.

The third goal of the research is to measure the extent to which Blockchain technology has been adopted within Malaysia's IoT ecosystem. While the study found a positive correlation between Blockchain adoption and the IoT ecosystem's growth, it seems that the study did not provide a direct measure of adoption in terms of percentages or specific metrics. Nevertheless, valuable insights were gained regarding adoption trends, particularly through an analysis of perceived adoption levels, which is a common method in both social science and technology adoption research.

Adoption Measurement: The research utilized Spearman's correlation to examine the relationship between Blockchain adoption and the IoT ecosystem. The resulting positive correlation coefficient of 0.528 suggests a moderate to strong link between the two variables, meaning that greater Blockchain adoption in IoT applications corresponds with a more developed IoT ecosystem in Malaysia. Although this does not offer a direct numerical measure of adoption (such as percentages or other adoption metrics), it does reveal a clear connection between adoption trends and the success of the ecosystem.

Providing Context: In technology adoption research, perceived trends—often based on individuals' attitudes, perceptions, or behaviors—are frequently used as key indicators, even when exact adoption figures are not available. Therefore, the study's findings align with the idea that adoptability plays a crucial role in the development of Malaysia's IoT ecosystem, even if precise adoption rates were not explicitly provided.

4.8.4 Mapping the Research Findings to the Research Problem and Research Questions

The findings of this study are directly aligned with the research problem and research questions, offering insights into the ways Blockchain technology could address the challenges faced by Malaysia's IoT ecosystem. Below is a detailed analysis of how the research findings correlate with the research problem and research questions.

Research Problem: IoT Infrastructure Challenges in Malaysia

Challenges in IoT Infrastructure: The research identifies several challenges with the existing centralized server-client model in Malaysia's IoT infrastructure, including issues related to scalability, high costs, and interoperability. These limitations hinder the growth and performance of IoT networks, particularly as the number of connected devices increases.

Blockchain's Potential Solution: The study highlights how Blockchain technology provides a decentralized alternative to the traditional infrastructure, offering potential solutions for cost reduction, scalability, security, and interoperability. Blockchain's ability to enable distributed networks without relying on central servers plays the key role to addressing some of the core challenges within IoT ecosystems in Malaysia.

How the Research Findings Answer This:

The study's findings affirm that Blockchain technology could play a significant role in overcoming issues within Malaysia's IoT ecosystem. A positive correlation between Blockchain adoption and IoT ecosystem success suggests that Blockchain may resolve challenges like scalability, cost-efficiency, and network reliability. The ordinal regression analysis revealed that awareness, usefulness, and adoptability of Blockchain are all strongly linked with the development of IoT networks, supporting Blockchain's potential to resolve infrastructure-related issues like scalability and security.

<u>Research Question 1:</u> How do IoT developers in Malaysia perceive the usefulness of Blockchain technology in addressing key challenges within IoT?

Research Problem Connection: The research problem points to the need for addressing issues like high infrastructure costs, scalability, and security within Malaysia's IoT ecosystem. However, the perceived usefulness of Blockchain in solving these problems has yet to be fully explored.

How the Research Findings Answer This: The study assesses how IoT developers in Malaysia perceive the usefulness of Blockchain, showing a positive correlation ($r = 0.486$) between usefulness and IoT ecosystem success. This indicates that developers view Blockchain as an effective solution to challenges such as security, scalability, and operational efficiency. The analysis also supports the idea that Blockchain is valued by developers for its ability to decentralize control, improve security, and automate processes (such as with smart contracts), addressing the inefficiencies of traditional centralized architectures.

<u>Research Question 2:</u> What is the current level of awareness and understanding of Blockchain technology among IoT professionals in Malaysia?

Research Problem Connection: The research problem highlights that Blockchain awareness is limited among IoT professionals in Malaysia, which impedes its broader adoption.

How the Research Findings Answer This: The study measures awareness of Blockchain and finds a moderate positive correlation (r = 0.467) between awareness of Blockchain and IoT ecosystem success. While awareness is still in the early stages, there is a growing understanding of Blockchain's potential for IoT development. The findings suggest that increasing awareness is critical to driving wider adoption and overcoming infrastructure challenges in the IoT sector.

<u>Research Question 3:</u> What are the current adoption trends of Blockchain technology within the Malaysian IoT ecosystem?

Research Problem Connection: The research problem emphasizes the need for Blockchain adoption to address challenges like high infrastructure costs, security issues, and data management within the IoT ecosystem. However, the exact rate of Blockchain adoption in Malaysia's IoT sector remains unclear.

How the Research Findings Answer This: Although the study does not provide a precise figure for the adoption rate, it highlights a moderate positive correlation ($r = 0.528$) between adoptability and the success of the IoT ecosystem. This indicates that increasing Blockchain adoption is positively influencing the development of Malaysia's IoT networks. The findings imply that Blockchain adoption is on the rise, even though the exact metrics are not directly quantified. The statistical significance of the correlations supports the idea that adoptability is a key driver of IoT success.

<u>How the Findings Address the Research Problem and Questions</u>

The research problem regarding scalability, cost, and security challenges in Malaysia's IoT infrastructure is addressed by the finding that Blockchain adoption (in terms of usefulness, awareness, and adoptability) correlates positively with IoT ecosystem success. Blockchain's decentralized features and benefits, such as enhanced security and cost-effectiveness, make it a promising solution to the infrastructure problems highlighted in the research problem. Whereas the research questions related to the perceived usefulness, awareness, and adoption trends of Blockchain in Malaysia's IoT ecosystem are answered by showing positive correlations between these factors and the development of the IoT ecosystem. The findings offer valuable insights into how IoT professionals perceive the usefulness of Blockchain, the growing awareness of its potential, and the role adoptability plays in advancing IoT infrastructure.

While the study does not directly quantify Blockchain adoption rates, it establishes a strong connection between Blockchain's potential and the improvement of Malaysia's

IoT ecosystem, thereby fulfilling the third research hypothesis and answering the key research questions.

4.8.5 Comparing TAM and Yaqoob's Model

The TAM model used in this research is primarily concerned with individual users' perceptions of usefulness and ease of use, which directly impact the user's intention to adopt the technology. Whereas Yaqoob's model, in contrast, likely includes a broader range of factors, such as organizational, regulatory, and industry-specific influences, alongside individual perceptions. It may also highlight issues like security and interoperability in the IoT space. TAM focuses on personal adoption decisions and the direct relationship between technology perception and user behavior, primarily targeting individual-level experiences. While Yaqoob's model, however, could offer a more comprehensive perspective on technology adoption, considering a broader set of factors like institutional and environmental influences, market conditions, and security concerns, especially in the IoT context.

In this study, TAM examines how IoT professionals in Malaysia perceive Blockchain's usefulness and its integration into existing IoT frameworks, focusing on individual decision-making and technology perception. Whereas If Yaqoob's model were applied to Blockchain and IoT adoption, it might explore industry-wide trends, including market readiness, regulatory influences, and interoperability challenges, in addition to individual perceptions of Blockchain.

TAM primarily concentrates on the individual's views on technology use, leaving out broader organizational or external influences. While Yaqoob's model, however, could account for key factors such as trust, security concerns, device interoperability, and regulatory compliance, all of which are significant in the IoT and Blockchain context. Both models address the concept of technology adoption, but they differ in their scope and focus. TAM is more centred on individual acceptance and highlights perceived usefulness and ease of use, while Yaqoob's model likely offers a more comprehensive view, incorporating external factors like security, trust, and regulatory influences, particularly important for IoT environments. The TAM model is utilized to investigate Blockchain adoption within Malaysia's IoT ecosystem, focusing on individual-level perceptions. Meanwhile, Yaqoob's model might consider these factors in a wider organizational or industry context, offering a more macro-level understanding of adoption trends.

4.9 Summary of the Chapter

The findings of the study are presented in this chapter, wherein a concise explanation of the figures and tables is provided. The chapter commenced with a concise introduction, succeeded by an elucidation of the response rate. The chapter additionally provided an overview of the demographic characteristics of the participants, the descriptive statistics, the reliability of the constructs, and the results of the correlation coefficient analysis. It also presented the findings regarding the ordinal regression of the independent variable in relation to the dependent variable (indicating a direct relationship). Lastly, the chapter provided a summary of its key points.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1 Introduction

This chapter serves as the concluding section of the research study, whereby the primary outcomes and discoveries of the investigation are discussed. The study's findings were further examined in terms of its managerial and theoretical implications, as well as the limitations of the study. Additionally, ideas for future research directions were provided.

5.2 Recapitulation of Study

The main objective of this research was to investigate how Blockchain technology could potentially help overcome the infrastructure-related challenges faced by Malaysia's IoT ecosystem, with a focus on issues such as scalability, security, cost, and interoperability. This study aimed to address the following research questions:

1. How do IoT developers in Malaysia perceive the usefulness of Blockchain technology in addressing key challenges within IoT?
2. What is the current level of awareness and understanding of Blockchain technology among IoT professionals in Malaysia?
3. What are the current adoption trends of Blockchain technology within the Malaysian IoT ecosystem?

The survey analysis yielded several important findings:

Perceived Usefulness of Blockchain: The results indicated a positive relationship between the perceived usefulness of Blockchain and the success of Malaysia's IoT ecosystem. IoT professionals regarded Blockchain as a viable solution to address critical challenges like scalability, security, and operational inefficiencies. Its decentralized nature was particularly appreciated for enhancing security and reducing reliance on centralized servers.

Awareness of Blockchain: While awareness of Blockchain technology among IoT professionals in Malaysia was still developing, there was a moderate positive correlation between awareness and the success of the IoT ecosystem. This suggests that raising awareness could play a pivotal role in speeding up Blockchain adoption and overcoming infrastructure obstacles in the IoT sector.

Adoption Trends: Although precise adoption rates were not provided, the findings indicated a moderate positive correlation between Blockchain adoption and IoT ecosystem success. This points to a growing trend of Blockchain integration within Malaysia's IoT sector. However, the adoption process remains gradual, and further initiatives are needed to accelerate its widespread implementation.

Addressing the Research Gap

This study effectively addressed several gaps in the existing literature:

Blockchain's Role in IoT Infrastructure: Prior to this research, there was a lack of detailed exploration into how Blockchain could specifically address the infrastructural challenges of IoT ecosystems, especially within the context of Malaysia. This study fills that gap by offering insights into how Blockchain can help overcome issues such as scalability, cost, and security.

Perception of Blockchain Among IoT Professionals: Another gap in the literature was the insufficient understanding of how IoT professionals perceive Blockchain's usefulness and potential for adoption. This study contributes empirical evidence, revealing that IoT professionals in Malaysia recognize Blockchain as a promising solution for overcoming challenges in their field, though awareness and adoption are still in the early stages.

Blockchain Adoption Trends in Malaysia's IoT Ecosystem: There was limited research on the current state of Blockchain adoption within Malaysia's IoT sector. This study provides important data showing that, while Blockchain adoption is still in its early phases, it is having a positive impact on the development of IoT networks in Malaysia.

In line with the study's objectives, a quantitative research methodology was adopted to assess various ideas and explore the relationships between different constructs. The sample consisted of individual developers from MDEC-listed ICT/IT firms in Malaysia. Of the survey questionnaires distributed, 433 were returned, with 349 deemed valid for inclusion in the analysis. The focus of the study was on the integration of Blockchain technology within these firms, particularly examining the influence of factors like usefulness, awareness, and the adoption rate of Blockchain technology.

The data analysis for this study was conducted using SPSS version 26, a software commonly used in social science research. Various statistical techniques were employed, including the analysis of demographic characteristics, descriptive statistics, reliability testing, correlation analysis, and ordinal regression. The sample for the study comprised Blockchain and IoT developers from ICT/IT firms across Malaysia. The descriptive data indicates generally positive perceptions of Blockchain technology within Malaysia's IoT sector. Respondents rated the technology's usefulness highly (mean: 3.19–3.62), with growing awareness (mean: 3.20–3.50) also noted. However, the adoption rate was more moderate (mean: 3.18–3.26), suggesting that while there is increasing recognition of Blockchain's potential, its actual implementation is still in the early stages. This gap points to a promising outlook for future adoption but also highlights the need for additional efforts to accelerate its integration into the IoT ecosystem.

Reliability analysis showed that the constructs were highly reliable, with Cronbach's alpha values of 0.913 for IoT ecosystem, 0.917 for adoption rate, 0.891 for awareness, and 0.887 for usefulness, all surpassing the threshold set by Field (2005). Correlation analysis revealed that the adoption rate of Blockchain had the strongest impact (0.528) on the IoT ecosystem, followed by usefulness (0.486) and awareness (0.467). Despite this variation, all constructs showed positive associations with the IoT ecosystem.

5.3 Research Contributions

This research study has made both theoretical and practical contributions to the existing body of literature on the willingness of ICT/IT software firms and developers to adopt Blockchain technology.

5.3.1 Theoretical Contributions

This thesis makes significant theoretical contributions by examining the role and potential of Blockchain technology in the IoT landscape, with a particular focus on Malaysia. It fills an existing gap in the literature regarding the convergence of IoT and Blockchain, offering fresh perspectives on how Blockchain can address critical challenges within IoT infrastructure. The study extends the well-known Technology Acceptance Model (TAM) by applying it to the specific domain of Blockchain technology within IoT systems. Although TAM has been widely used to understand the adoption of general technologies, this research takes a more focused approach, examining how IoT professionals perceive Blockchain's ease of use, usefulness, and its ability to address pressing issues like scalability, security, and cost-effectiveness. Furthermore, the research contributes to the growing body of knowledge by illustrating how Blockchain can be leveraged to resolve key challenges within IoT ecosystems, particularly regarding infrastructure, security, and scalability. The findings reinforce the notion that Blockchain's decentralized nature and inherent security features make it an ideal candidate for addressing some of the most pressing problems facing IoT networks.

The study also offers valuable insights into the perspectives of IoT developers in Malaysia, providing a clearer understanding of their views on Blockchain technology. It contributes to the literature on technology adoption by examining how developers evaluate and make decisions about integrating new technologies like Blockchain into their IoT systems. This thesis enhances the theoretical framework for Blockchain adoption by linking essential constructs—such as awareness, perceived usefulness, and overall adoption—with the success and development of IoT ecosystems. It emphasizes that raising awareness is a crucial first step in fostering the adoption of Blockchain and demonstrates how these factors interact to influence the broader acceptance and integration of Blockchain in IoT applications.

5.3.2 Practical Contributions

This thesis offers significant practical contributions that can benefit IoT sector in Malaysia and contribute to the broader adoption of Blockchain technology in real-world applications. The results are intended to assist decision-makers, IoT professionals, and policymakers in effectively incorporating Blockchain into IoT infrastructures to solve existing challenges. The research underscores the need for increasing Blockchain awareness among IoT developers in Malaysia. Given that greater awareness is linked to better adoption and success, the thesis suggests expanding educational programs, workshops, and resources to foster greater familiarity with Blockchain in the IoT community.

The findings of the study indicate that Blockchain could help resolve some of the infrastructure challenges facing IoT in Malaysia. Policymakers can leverage this information to shape policies that encourage Blockchain adoption, such as creating regulatory frameworks, providing incentives, or supporting collaborative research in Blockchain and IoT. The study suggests that Blockchain adoption positively influences the success of the IoT ecosystem. Industry leaders can use these insights to integrate Blockchain solutions that enhance the efficiency, security, and resilience of IoT networks. This study emphasizes the importance of Blockchain in IoT development, not just as a technical solution, but also as a catalyst for cross-sector collaboration. The findings suggest that close cooperation between technology developers, IoT manufacturers, and policymakers will be critical for widespread Blockchain adoption in the IoT ecosystem.

5.4 Limitations of Study

One noteworthy constraint of this study is the lack of specific examination of the inherent security variances among various types of Blockchain. Although the research primarily centres around Blockchain technology and IoT ecosystem, it fails to provide a full analysis of the diverse levels of security and trustworthiness exhibited by individual Blockchains. Future study endeavours may entail an examination of the security qualities inherent in different Blockchains, with the aim of acquiring a more profound comprehension of their impact on individuals' intentions to adopt and organisations' general preparedness to embrace Blockchain technology.

5.5 Future Research Direction

While this study offers numerous valuable insights, it is important to acknowledge that there are still certain limitations that need to be addressed in future research. The scope of this study is restricted to ICT/IT software firms operating inside the Malaysian context. The potential consequence of this is a potential restriction on the applicability of the results to software companies operating in diverse nations or industries. Furthermore, it should be noted that the scope of this study is restricted to individuals in positions of authority and developers inside these organisations. Subsequent investigations might potentially incorporate the viewpoints of additional parties involved, such as employees or customers. Also, the framework's scope is kept to four aspects, exclusively assessing direct associations. Subsequent research endeavours may delve into supplementary factors that could enhance the readiness for Blockchain adoption within the IoT ecosystem, taking into account the potential effect of moderating and mediating variables.

5.6 Conclusion

The development of the conceptual framework was informed by a comprehensive review of the existing literature on the deployment of Blockchain technology within the IoT ecosystem. A comprehensive selection of established literatures was examined to identify significant and pertinent elements. These components were subsequently incorporated into a meticulously constructed study framework, with the aim of exploring the impact of each postulated link on the ICT/IT software industry. The objective of this study was to validate the research framework required for evaluating the readiness of ICT/IT software enterprises in Malaysia to embrace Blockchain technology. The research framework highlighted the importance of usefulness, awareness, adoptability rate of Blockchain with IoT within the ecosystem characteristics and challenges pertaining to the adoption and deployment.

REFERENCES

Adhikari, N., & Ramkumar, M. (2023). IoT and Blockchain Integration: Applications, Opportunities, and Challenges. Network, 3(1), 115-141.

Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018). Applications of blockchains in the Internet of Things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 21(2), 1676-1717.

Ali, S. A., Elsaid, S. A., Ateya, A. A., ElAffendi, M., & El-Latif, A. A. A. (2023). Enabling Technologies for Next-Generation Smart Cities: A Comprehensive Review and Research Directions. Future Internet, 15(12), 398.

Aliaga, M. and Gunderson, B., (2006). Interactive statistics. Upper Saddle River, N.J.: Pearson Prentice Hall.

Anderson, J. C., and Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. Psychological bulletin, 103(3), 411.

Andreas Antonopoulos (2020). Bitcoin security model: trust by computation. O'Reilly Radar. Retrieved October 4, 2020.

Anthony, B. J. Majid, M, A. and Romli, A. (2018). "An empirical study on predictors of green sustainable software practices in Malaysian electronic industries," Journal of Information and Communication Technology, vol. 17, no. 11, pp. 347-391.

Antonopoulos, A. M. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. M 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc.

Apat, H. K., Sahoo, B., Mohanty, S., Mukul, M., & Barik, R. K. (2023). A Blockchain assisted fog computing framework for secure data sharing mechanism in smart home. In 2023 IEEE International Conference on Contemporary Computing and Communications (InC4) (Vol. 1, pp. 1-6). IEEE.

Apuke, O.D. (2017). Quantitative Research Methods: A Synopsis Approach. Kuwait chapter of Arabian Journal of Business & Management Review, 6, 40-47.

Arshad, Q. U. A., Khan, W. Z., Azam, F., Khan, M. K., Yu, H., & Zikria, Y. B. (2023). Blockchain-based decentralized trust management in IoT: systems, requirements and challenges. Complex & Intelligent Systems, 1-22.

Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Wills, G. (2018). Blockchain with internet of things: Benefits, challenges, and future directions. Int. J. Intell. Syst. Appl, 40–48.

Attia, O.; Khoufi, I.; Laouiti, A.; Adjih, C. (2019). An IoT-blockchain architecture based on hyperledger framework for healthcare monitoring application. In

Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain; pp. 1–5.

Atzori, L.; Iera, A.; Morabito, G. (2010). The internet of things: A survey. Comput. Netw., 54, 2787–2805.

Awang, Z. A. (2012). Handbook on SEM Structural Equation Modelling: SEM Using AMOS Graphic (5th ed.). Kota Baru: Universiti Teknologi Mara Kelantan.

Bahga, A.; Madisetti, V.K. (2016). Blockchain platform for industrial internet of things. J. Softw. Eng. Appl. 9, 533–546.

Bali, M. S., Gupta, K., & Malik, S. (2022). Integrating IoT with blockchain: a systematic review. IoT and Analytics for Sensor Networks: Proceedings of ICWSNUCA 2021, 355-369.

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. Journal of personality and social psychology, 51(6), 1173.

Bartlett, M. S. (1954). A note on the multiplying factors for various χ 2 approximations. Journal of the Royal Statistical Society. Series B (Methodological), 296-298.

Bell, E., Bryman, A., & Harley, B. (2018). Business Research Methods. Oxford, England: Oxford University Press.

Biswas, K.; Muthukkumarasamy, V. (2016). Securing Smart Cities Using Blockchain Technology. In Proceedings of the 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, Australia; pp. 1392–1393.

Bitcoin, (2010), en.bitcoin.it, [Online]. Available: https://en.bitcoin.it/wiki/Laszlo_Hanyecz#Pizza. Retrieved November 25, 2020.

Bourn, Douglas. (2015). The Theory and Practice of Development Education: A Pedagogy for Global Social Justice. New York: Routledge. pp 222.

Bradburn, N., Sudman, S., & Wansink, B. (2004). Asking questions: The definitive guide to questionnaire design-For market research, political polls, and social and health questionnaires (Rev. ed.). Jossey-Bass.

Brennan, P. F., & Hays, B. J. (1992). Focus on psychometrics the kappa statistic for establishing interrater reliability in the secondary analysis of qualitative clinical data. Research in nursing & health, 15(2), 153-158.

Bryman, A. and Bell, E. (2011) Business Research Methods. 3rd Edition, Oxford University Press, Oxford.

Burns, N. and Grove, S.K. (2005). The Practice of Nursing Research: Conduct, Critique and Utilization. 5th Edition, Elsevier Saunders, Missouri.

Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. White Pap. 3, 37.

Butun, I. (2020). Industrial IoT: Challenges, Design Principles, Applications, and Security; Springer Nature: Cham, Switzerland

Butun, I.; Österberg, P. (2019). Detecting intrusions in cyber-physical systems of smart cities: Challenges and directions. In Secure Cyber-Physical Systems for Smart Cities; IGI Global: Goteborg, Sweden; pp. 74–102.

Butun, I.; Österberg, P.; Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Commun. Surv. Tutor. 22, 616–644.

Butun, I.; Sari, A.; Österberg, P. (2020). Hardware Security of Fog End-Devices for the Internet of Things. Sensors, 20, 5729.

Byrne, B.M. (2010). Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming (2nd Edition). New York: Taylor and Francis Group Publication

Cavana, R., Delahaye, B., & Sekeran, U. (2001). Applied business research: Qualitative and quantitative methods. John Wiley & Sons.

Celik, Y., Petri, I., & Barati, M. (2023). Blockchain supported BIM data provenance for construction projects. Computers in Industry, 144, 103768.

Chaganti, R., Bhushan, B., & Ravi, V. (2023). A survey on Blockchain solutions in DDoS attacks mitigation: Techniques, open challenges and future directions. Computer Communications, 197, 96-112.

Chatziamanetoglou, D., & Rantos, K. (2023). Blockchain-Based Security Configuration Management for ICT Systems. Electronics, 12(8), 1879.

Cheng, C. L. Shalabh, G. Garg, (2014). Coefficient of determination for multiple measurement error models, Journal of Multivariate Analysis, 126, 137-152.

Cheng, M.-T., She, H.-C., & Annetta, L. A. (2014). Game immersion experience: Its hierarchical structure and impact on game-based science learning. Journal of Computer Assisted learning. doi:10.1111/jcal.12066.

Christidis, K. and G. S. Member, (2016). Blockchains and Smart Contracts for the Internet of Things, IEEE Access, vol. 4, pp. 2292–2303.

Churchill, G. and D. Iacobucci, (2002). Marketing Research, Methodological Foundations. 6th Edition, Harcourt Publishing, London.

Churchill, G. and D. Iacobucci, (2005). Marketing Research, Methodological Foundations. 8th Edition, Harcourt Publishing, London.

Churchill, G.A. (1979). "A Paradigm for Developing Better Measures of Marketing Constructs", Journal of Marketing Research, no. 16, pp. 64-73.

Churchill, J. D., Galvez, R., Colcombe, S., Swain, R. A., Kramer, A. F., & Greenough, W. T. (2002). Exercise, experience and the aging brain. Neurobiology of aging, 23(5), 941-955.

Clason, D. L., and Dormody, T. J. (1994). Analyzing data measured by individual Likert-type items. Journal of agricultural education, 35(4), 4.

Coakes, S. J., & Steed, L. (2007). SPSS Version 14.0 for Windows: Analysis with out anguish. JohnWiley & Sons Australia Ltd., Australia, 3(1), 15.

Cohen, J. (1988). Statistical power analysis for the behavioural sciences 2nd ed Lawrence Erlbaum Associates. Hillsdale, NJ.

Collis, J., & Hussey, R. (2009). Business research: A practical guide for undergraduate and postgraduate students. Palgrave macmillan.

Comrey, A. L., & Lee, H. B. (2013). A first course in factor analysis (2nd ed.). Lawrence Erlbaum Associates, Inc.

Coolican, H. (1990). Research methods and statistics in psychology. Hodder & Stoughton Educational.

Costello, K. (2019). Gartner survey reveals blockchain adoption combined with IOT adoption is booming in the U.S. Gartner. https://www.gartner.com/en/newsroom/press-releases/2019-12-12-gartner-survey-reveals-blockchain-adoption-combined-with-iot-adoption-is-booming-in-the-us#:~:text=IoT%20Implementers%20Are%20Big%20on,technologies%20together%20in%20various%20projects.

Creswell, J. W. (2013). Qualitative Inquiry & Research Design: Choosing among Five Approaches (3rd ed.). Thousand Oaks, CA: SAGE.

Creswell, J. W., Hanson, W. E., Clark Plano, V. L., & Morales, A. (2007). Qualitative research designs: Selection and implementation. The counseling psychologist, 35(2), 236-264.

Creswell, J., & Plano Clark, V. (2007). Designing and Conducting Mixed Methods Research. Thousand Oaks, CA: Sage.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. psychometrika, 16(3), 297-334.

Dai, Y.; Xu, D.; Maharjan, S.; Chen, Z.; He, Q.; Zhang, Y. (2019). Blockchain and deep reinforcement learning empowered intelligent 5G beyond. IEEE Netw. 33, 10–17.

Davis, L. L. (1992). Instrument review: Getting the most from a panel of experts. Applied nursing research, 5(4), 194-197.

Dinh C Nguyen, Pubudu N Pathirana, Ming Ding, and Aruna Seneviratne. (2019). Integration of blockchain and cloud of things: Architecture, applications and challenges. arXiv preprint arXiv:1908.09058.

Dolhopolov, A., Castelltort, A., & Laurent, A. (2023). Implementing a Blockchain-Powered Metadata Catalog in Data Mesh Architecture. In International Congress on Blockchain and Applications (pp. 348-360). Cham: Springer Nature Switzerland.

Dutta, P., Chavhan, R., Gowtham, P., & Singh, A. (2023, January). The individual and integrated impact of Blockchain and IoT on sustainable supply chains: A systematic review. In Supply Chain Forum: An International Journal (Vol. 24, No. 1, pp. 103-126). Taylor & Francis.

Emma Bell; (2018). Alan Bryman. Business research methods. Oxford University Press.

Falayi, A., Wang, Q., Liao, W., & Yu, W. (2023). Survey of Distributed and Decentralized IoT Securities: Approaches Using Deep Learning and Blockchain Technology. Future Internet, 15(5), 178.

Farahani, B., Firouzi, F. and Luecking, M., (2021). The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. Journal of Network and Computer Applications, 177, p.102936.

Fatma Ellouze, Ghofrane Fersi, and Mohamed Jmaiel. (2020). Blockchain for internet of medical things: A technical review. In International Conference on Smart Homes and Health Telematics, pages 259–267. Springer.

Fernandez-Carames, T.M.; Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. IEEE Access, 6, 32979–33001

Field, A. P. (2005). Is the meta-analysis of correlation coefficients accurate when population correlations vary?. Psychological methods, 10(4), 444.

Fink, A. (2017). How to Conduct Surveys: A Step-by-Step Guide. (6ed). Los Angeles: Sage

Geist, D. (2016). Using the Bitcoin Blockchain as a Botnet Resilience Mechanism.

Govindan, K., Jain, P., Singh, R. K., & Mishra, R. (2024). Blockchain technology as a strategic weapon to bring procurement 4.0 truly alive: Literature review and future research agenda. Transportation Research Part E: Logistics and Transportation Review, 181, 103352.

Gugueoth, V., Safavat, S., Shetty, S., & Rawat, D. (2023). A review of IOT security and privacy using decentralized blockchain techniques. Computer Science Review, 50, 100585.

Guilford, J. P. (1965). The minimal phi coefficient and the maximal phi. Educational and psychological measurement, 25(1), 3-8.

Hair, J. F., Black, W. C., Babin, B. J. et al. (2010). Multivariate Data Analysis (7th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). Multivariate data analysis 6th Edition. Pearson Education

Hair, J. F., Gabriel, M., and Patel, V. (2014). AMOS covariance-based structural equation modeling (CB-SEM): Guidelines on its application as a marketing research tool. Brazilian Journal of Marketing, 13(2).

Harris, L. R., and Brown, G. T. (2010). Mixing interview and questionnaire methods: Practical problems in aligning data. Practical Assessment, Research, and Evaluation, 15(1), 1.

Heller, B.; Sherwood, R.; McKeown, N. (2012) The controller placement problem. ACM SIGCOMM Comput. Commun. Rev. 42, 473–478.

Henseler, J., Ringle, C. M., and Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In New challenges to international marketing. Emerald Group Publishing Limited.

Hewa, T.; Braeken, A.; Ylianttila, M.; Liyanage, M. (2020). Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT. In Proceedings of the 8th IEEE International Conference on Communications and Networking (IEEE ComNet'2020), Hammamet, Tunisia.

Horn, J. L. (1965). A rationale and test for the number of factors in factor analysis. Psychometrika, 30, 179-185.

Hubbard, R., & Allen, S. J. (1987). An empirical comparison of alternative methods for principal component extraction. Journal of Business Research, 15(2), 173-190.

Hunt, S. D., Sparkman Jr, R. D., & Wilcox, J. B. (1982). The pretest in survey research: Issues and preliminary findings. Journal of marketing research, 19(2), 269-273.

IBM, (2015). ADEPT: An IoT Practitioner Perspective.

Issa, W., Moustafa, N., Turnbull, B., Sohrabi, N., & Tari, Z. (2023). Blockchain-based federated learning for securing internet of things: A comprehensive survey. ACM Computing Surveys, 55(9), 1-43.

Jackson, A., Spiegler, V. L., & Kotiadis, K. (2024). Exploring the potential of blockchain-enabled lean automation in supply chain management: A systematic literature review, classification taxonomy, and future research agenda. Production Planning & Control, 35(9), 866-885.

Jahid, A., Alsharif, M. H., & Hall, T. J. (2023). The convergence of Blockchain, IoT and 6G: potential, opportunities, challenges and research roadmap. Journal of Network and Computer Applications, 103677.

Jnr, B. A., Sylva, W., Watat, J. K., & Misra, S. (2023). A Framework for Standardization of Distributed Ledger Technologies for Interoperable Data Integration and Alignment in Sustainable Smart Cities. Journal of the Knowledge Economy, 1-44.

Johnson, B., & Christensen, L. (2000). Educational research: Quantitative and qualitative approaches. Allyn & Bacon.

Joshi, A., Kale, S., Chandel, S., and Pal, D. K. (2015). Likert Scale: Explored and Explained. British Journal of Applied Science and Technology, 7(4), 396–452.

Junqin Huang, Linghe Kong, Guihai Chen, Min-You Wu, Xue Liu, and Peng Zeng. (2019). Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics, 15(6):3680–3689.

Kaiser, H. F. (1974). An index of factorial simplicity. psychometrika, 39(1), 31-36.

Karame, G. (2016). On the security and scalability of bitcoin's blockchain. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria; pp. 1861–1862.

Kaur, B., Dadkhah, S., Shoeleh, F., Neto, E. C. P., Xiong, P., Iqbal, S., ... & Ghorbani, A. A. (2023). Internet of things (IoT) security dataset evolution: Challenges and future directions. Internet of Things, 100780.

Khan, P.W.; Byun, Y. A. (2020). Blockchain-Based Secure Image Encryption Scheme for the Industrial Internet of Things. Entropy; 22, 175.

Kiran, M., Ray, B., Hassan, J., Kashyap, A., & Chandrappa, V. Y. (2024). Blockchain based secure Ownership Transfer Protocol for smart objects in the Internet of Things. Internet of Things, 25, 101002.

Kitchenham BA, Mendes E, Travassos GH (2007) Cross versus within-company cost estimation studies: a systematic review. IEEE Trans Softw Eng 33(5):316–329

Kitchenham, B. and Charters, S. (2007). Guidelines for Performing Systematic Literature Reviews in Software Engineering, Technical Report EBSE 2007-001, Keele University and Durham University Joint Report.

Kothari, C. R. (2004). Sample size determination. Research Methodology. New Age International Publications, 1, 74-1.

Kothari, C., Kumar, R., and Uusitalo, O. (2014). Research Methodology 3rd Edition. New Age International (p. 418).

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. Educational and psychological measurement, 30(3), 607-610.

Ku Ruhana Ku-Mahamud,Mazni Omar,Nur Azzah Abu Bakar and Ishola Dada Muraina, 2019). "Awareness, Trust, and Adoption of Blockchain Technology and Cryptocurrency among Blockchain Communities in Malaysia," International Journal on Advanced Science, Engineering and Information Technology, vol. 9, no. 4, pp. 1217-1222 Available: http://dx.doi.org/10.18517/ijaseit.9.4.6280.

Kureshi, F., Makwana, D., Bodkhe, U., Tanwar, S., & Chaturvedi, P. (2023). Blockchain Based Humans-Agents Interactions/Human-Robot Interactions: A Systematic Literature Review and Research Agenda. Robotic Process Automation, 139-165.

Lantz, B. (2013). The impact of sample non-normality on ANOVA and alternative methods. British Journal of Mathematical and Statistical Psychology, 66(2), 224-244.

Lanxiang Chen, Wai-Kong Lee, Chin-Chen Chang, Kim-Kwang Raymond Choo, and Nan Zhang. (2019). Blockchain based searchable encryption for electronic health record sharing. Future Generation Computer Systems, 95:420–429.

Lao, L.; Li, Z.; Hou, S.; Xiao, B.; Guo, S.; Yang, Y. (2020). A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. ACM Comput. Surv. (CSUR), 53, 1–32.

Latif, S.; Idrees, Z.; Ahmad, J.; Zheng, L.; Zou, Z. (2020). A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. J. Ind. Inf. Integr, 21, 100190

Lee, D. and Park, N., (2021). Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree. Multimedia Tools and Applications, 80, pp.34517-34534.

Lee, S.K.; Bae, M.; Kim, H. (2017) Future of IoT networks: A survey. Appl. Sci

Liu, Y., Wang, J., Yan, Z., Wan, Z., & Jäntti, R. (2023). A survey on blockchain-based trust management for Internet of Things. IEEE Internet of Things Journal, 10(7), 5898-5922.

Luo, Y.Y. (2021). Research on the Methods of Management of University Students in the Big Data Age. Open Access Library Journal, 8, 1-6.

Lynn, M. R. (1986). Determination and quantification of content validity. Nursing research, 35(6), 382-386.

Maayan, G. D (2020). The IoT Rundown For 2020: Stats, Risks, and Solutions. [Online]. Available: https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.aspx Retrieved August 17, 2020

Malhotra, N. & Birks, D. (2007) Marketing Research: an applied approach: 3rd European Edition, Harlow, UK. Pearson Education, 835pp.

Mangur, V. (2020). How much does IoT development cost - 2020. [Online]. Available: https://thinkmobiles.com/blog/iot-app-development-cost/. Retrieved October 4, 2020.

Md Abdur Rahman, Md Mamunur Rashid, M Shamim Hossain, Elham Hassanain, Mohammed F Alhamid, and Mohsen Guizani. (2019). Blockchain and iot-based cognitive edge framework for sharing economy services in a smart city. IEEE Access, 7:18611–18621.

MDEC. List of MSC Malaysia Status Companies. (2022). Available online: https://mdec.my/what-we-offer/msc-malaysia/

Merkel, D. Docker: (2014). Lightweight Linux containers for consistent development and deployment. Linux J., 2

Mettler, M., (2016). Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom) (pp. 1-3). IEEE.

Mingxin Ma, Guozhen Shi, and Fenghua Li. (2019). Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the iot scenario. IEEE Access, 7:34045–34059.

Minhaj Ahmad Khan and Khaled Salah. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82:395–411, 2018

Muhammad Habib ur Rehman, Ibrar Yaqoob, Khaled Salah, Muhammad Imran, Prem Prakash Jayaraman, and Charith Perera. (2019) The role of big data analytics in industrial internet of things. Future Generation Computer Systems, 99:247–259.

Mutlag, A.A.; Abd Ghani, M.K.; Arunkumar, N.A.; Mohammed, M.A.; Mohd, O. (2019). Enabling technologies for fog computing in healthcare IoT systems. Future Gener. Comput. Syst., 90, 62–78.

Naaz, R., Saxena, A. K., & Shah, P. K. (2023, February). Blockchain technology's overview: Consensus, architecture and future trends. In AIP Conference Proceedings (Vol. 2427, No. 1). AIP Publishing.

Nakamoto S., (2008), Bitcoin: A Peer-to-Peer Electronic Cash System, bitcoin.org, [Online]. Available: https://bitcoin.org/bitcoin.pdf. Retrieved November 17, 2020.

Narayan, G., Haveri, P., Rashmi, B., & Deewan, Y. (2024). A Framework for Data Provenance Assurance in Cloud Environment using Ethereum Blockchain: Data Provenance Assurance in Cloud using Blockchain. EAI Endorsed Transactions on Scalable Information Systems, 11(2).

Nils Siegfried, Tobias Rosenthal, Alexander Benlian. (2020). Blockchain and the industrial internet of things: A requirement taxonomy and systematic fit analysis. Technical report, Darmstadt Technical University, Department of Business Administration.

Norusis, M. (2003). SPSS 12.0 statistical procedures companion. Upper Saddle.

Norusis, M. J. (1992). SPSS for Windows: Professional Statistics User's Guide, Release 5.0. SPSS Incorporated.

Nuryyev, G.; Wang, Y.-P.; Achyldurdyyeva, J.; Jaw, B.-S.; Yeh, Y.-S.; Lin, H.-T.; Wu, L.-F. (2020). Blockchain Technology Adoption Behavior and Sustainability of the Business in Tourism and Hospitality SMEs: An Empirical Study. Sustainability, 12, 1256.

Ongaro, D.; Ousterhout, J. (2014). In search of an understandable consensus algorithm. In Proceedings of the 2014 USENIX Annual Technical Conference (USENIXATC 14), Philadelphia, PA, USA; pp. 305–319.

Osborne, J. W. (2017). Regression and linear modeling: best practices and modern methods. Thousand Oaks, CA: Sage.

Pallant, J. (2007). SPSS survival manual: A step by step guide to data analysis using SPSS for Windows, 3rd, New York, NY: McGraw-Hill.

Pallant, J. F., and Tennant, A. (2007). An introduction to the Rasch measurement model: an example using the Hospital Anxiety and Depression Scale (HADS). British Journal of Clinical Psychology, 46(1), 1-18.

Partha Pratim Ray, Dinesh Dash, Khaled Salah, and Neeraj Kumar. (2020) Blockchain for IoT -based healthcare: Background, consensus, platforms, and use cases. IEEE Sys Journ.

Peat J., & Barton B. (2005). Medical Statistics: A guide to data analysis and criti-cal appraisal. Blackwell Publishing

Peng, Z.; Wu, H.; Xiao, B.; Guo, S. (2019). VQL: Providing query efficiency and data authenticity in blockchain systems. In Proceedings of the 2019 IEEE 35th International Conference on Data Engineering Workshops (ICDEW), Macao, China; pp. 1–6.

Penrod, J., Preston, D. B., Cain, R. E., & Starks, M. T. (2003). A Discussion of Chain Referral as a Method of Sampling Hard-to-Reach Populations. Journal of Transcultural Nursing, 14(2), 100–107.

Perez, D., Xu, J. and Livshits, B., (2020). October. Revisiting transactional statistics of high-scalability blockchains. In Proceedings of the ACM Internet Measurement Conference (pp. 535-550).

Peši´c, S.; Radovanovi´c, M.; Ivanovi´c, M.; Toši´c, M.; Ikovi´c, O.; Boškovi´c, D. (2019). Hyperledger Fabric Blockchain as a Service for the IoT: Proof of

Concept. In Proceedings of the International Conference on Model and Data Engineering, Toulouse, France; pp. 172–183.

Petrucci, C.J. (2009). A primer for social worker researchers on how to conduct a multinomial logistic regression. Journal of Social Service Research, 35, 193-205.

Pituch, K. A., & Stevens, J. P. (2016). Applied Multivariate Statistics for the Social Sciences. 6th edn. New York and London.

Polit, D. F., & Beck, C. T. (2006). The content validity index: are you sure you know what's being reported? Critique and recommendations. Research in nursing & health, 29(5), 489-497.

Primavera De Filippi, Morshed Mannan, and Wessel Reijers. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society, 62:101284.

Qiheng Zhou, Huawei Huang, Zibin Zheng, and Jing Bian. (2020). Solutions to scalability of blockchain: A survey. IEEE Access, 8:16440–16455.

Qingqing, L.; Yuhong, F.; Queralta, J.P.; Gia, T.N.; Tenhunen, H.; Zou, Z.; Westerlund, T. (2019). Edge computing for mobile robots: multi-robot feature-based lidar odometry with FPGAs. In Proceedings of the 2019 Twelfth International Conference on Mobile Computing and Ubiquitous Network (ICMU), Kathmandu, Nepal; pp. 1–2.

Queralta, J.P.; Gia, T.N.; Tenhunen, H.; Westerlund, T. (2019). Collaborative mapping with ioe-based heterogeneous vehicles for enhanced situational awareness. In Proceedings of the 2019 IEEE Sensors App Symposium (SAS), Sophia Antipolis, France; pp. 1–6.

Queralta, J.P.; Qingqing, L.; Gia, T.N.; Truong, H.L.; Westerlund, T. (2020). End-to-End Design for Self-Reconfigurable Heterogeneous Robotic Swarms. arXiv.

Queralta, J.P.; Qingqing, L.; Zou, Z.; Westerlund, T. (2020). Enhancing Autonomy with Blockchain and Multi-Acess Edge Computing in Distributed Robotic Systems. In Proceedings of the Fifth International Conference on Fog and Mobile Edge Computing (FMEC), Paris, France.

Rahman, A., Islam, M. J., Band, S. S., Muhammad, G., Hasan, K., & Tiwari, P. (2023). Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. Digital Communications and Networks, 9(2), 411-421.

Rasinger, S. M. (2013). Quantitative research in linguistics: An introduction. A&C Black.

Razali, N.A.M.; Wan Muhamad, W.N.; Ishak, K.K.; Saad, N.J.A.M.; Wook, M.; Ramli, S. (2021). Secure Blockchain-Based Data-Sharing Model and Adoption among Intelligence Communities. IAENG Int. J. Comput. Sci., 48, 18–31.

Rejeb, A., Appolloni, A., Rejeb, K., Treiblmaier, H., Iranmanesh, M., & Keogh, J. G. (2023). The role of blockchain technology in the transition toward the circular economy: Findings from a systematic literature review. Resources, Conservation & Recycling Advances, 17, 200126.

Rejeb, A., Rejeb, K., Appolloni, A., Jagtap, S., Iranmanesh, M., Alghamdi, S., ... & Kayikci, Y. (2023). Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions. Internet of Things and Cyber-Physical Systems.

Rennie, D., Yank, V., and Emanuel, L. (1997). When authorship fails: a proposal to make contributors accountable. Jama, 278(7), 579-585.

Rifi, N., Rachkidi, E., Agoulmine, N. and Taher, N.C., (2017). Towards using blockchain technology for IoT data access protection. In 2017 IEEE 17th international conference on ubiquitous wireless broadband (ICUWB) (pp. 1-5). IEEE.

Robson, C. (2002). Real World Research: A Resource for Social Scientists and Practitioner-Researchers (2nd ed.). Oxford: Blackwell Publishers Ltd

Said El Kafhali, Chorouk Chahir, Mohamed Hanini, and Khaled Salah. (2019). Architecture to manage internet of things data using blockchain and fog computing. In Proceedings of the 4th International Conference on Big Data and Internet of Things, pages 1–8.

Salkind, N. J. (1997). Exploring Research. (3rd Ed.). New Jersey, Upper Saddle River, Prentice Hall, Inc.

Samaniego, M. and R. Deters, (2016). Blockchain as a Service for IoT, 2016 IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, pp. 433–436.

Samaniego, M.; Deters, R. (2016a). Using blockchain to push software-defined IoT components onto edge hosts. In Proceedings of the International Conference on Big Data and Advanced Wireless Technologies, Blagoevgrad, Bulgaria; pp. 1–9.

Saunders, M., Lewis, P., & Thornhill, A. (2003). Research Methods for Business Students (3rd ed.). England: Prentice Hall.

Sekaran, U. and Bougie, R. (2013) Research Methods for Business: A Skill-Building Approach. 6th Edition, Wiley, New York.

Sekaran, U., & Bougie, R. (2010). Research methods for business: A skill-building approach (5th ed.). Haddington: John Wiley & Sons.

Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill building approach. (7th ed.). john wiley & sons.

Shangping Wang, Yinglong Zhang, and Yaling Zhang. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access, 6:38437–38450.

Shankar, A., & Maple, C. (2023). Securing the Internet of Things-enabled smart city infrastructure using a hybrid framework. Computer Communications, 205, 127-135.

Shbair, W.M., Steichen, M. and François, J., (2018). Blockchain orchestration and experimentation framework: A case study of KYC. In IEEE/IFIP Man2Block 2018-IEEE/IFIP Network Operations and Management Symposium.

Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. (2019lee). Edge computing: Vision and challenges. IEEE Internet Yhings J, 3, 637–646

Simić, M., Sladić, G. and Milosavljević, B., (2017). A case study IoT and blockchain powered healthcare. Proc. ICET, pp.1-4.

Soldani, D. (2019). 5G and the Future of Security in ICT. In Proceedings of the 2019 29th International Telecommunication Networks and Applications Conference (ITNAC), Auckland, New Zealand; pp. 1–8.

Soumyashree S Panda, Utkalika Satapathy, Bhabendu K Mohanta, Debasish Jena, and Debasis Gountia. (2019). A blockchain based decentralized authentication framework for resource constrained IoT devices. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pages 1–6. IEEE.

Stallings, W. (2015). The Internet of Things: Network and Security Architecture, Internet Protoc. J., vol. 18, no. 4, pp. 2–24

Stanciu. A. (2017). Blockchain based distributed control system for Edge Computing, in 21st International Conference on Control Systems and Computer Science Blockchain, pp. 667–671

Steinskog DJ. (2007). A cautionary note on the use of the Kolmogorov-Smirnov test for normality. American Meteor Soc. 135:1151-7

Su, P.H.; Shih, C.S.; Hsu, J.Y.J.; Lin, K.J.; Wang, Y.C. (2014). Decentralized fault tolerance mechanism for intelligent IoT/M2M middleware. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea; pp. 45–50.

Suen, C.H.; Ko, R.K.; Tan, Y.S.; Jagadpramana, P.; Lee, B.S. (2013). S2logger: End-to-end data tracking mechanism for cloud data provenance. In Proceedings of the 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, Australia; pp. 594–602.

Tabachnick, B. G., & Fidell, L. S. (2007). Multivariate analysis of variance and covariance. Using Multivariate Statistics, 3, 402–407.

Thode HJ. (2002). Testing for normality. New York: Marcel Dekker.

Torkaman, A. and M. A. Seyyedi, (2016). Analyzing IoT Reference Architecture Models, Int. J. Comput. Sci. Softw. Eng. ISSN, vol. 5, no. 8, pp. 2409–4285.

Tseng, C. H., & Sim, D. (2021). Sample size planning for pilot studies. arXiv preprint arXiv:2105.05483.

Ucbas, Y., Eleyan, A., Hammoudeh, M., & Alohaly, M. (2023). Performance and scalability analysis of ethereum and hyperledger fabric. IEEE Access.

Ullah, N.; Alnumay, W.S.; Al-Rahmi, W.M.; Alzahrani, A.I.; Al-Samarraie, H. (2020). Modeling Cost Saving and Innovativeness forBlockchain Technology Adoption by Energy Management. Energies, 13, 4783.

Veena Pureswaran, S.P.; Nair, S.; Brody, P. (2015). Empowering the Edge-Practical Insights on a Decentralized Internet of Things. Available online: https://www.ibm.com/downloads/cas/2NZLY7XJ (accessed on 8 June 2023).

Vemula, K. (2023). AN END-TO-END DECENTRALIZED INTERNET OF THINGS (IOT) DATA MODEL.

Verma, H., & Arora, P. (2022). Applications and blockchain solution for Big Data Challenges. ECS Transactions, 107(1), 6905–6912.

Vilchez, P., Jacques, S., Freitag, F., & Meseguer, R. (2023). LoRaTRUST: Blockchain-Enabled Trust and Accountability Service for IoT Data. Electronics, 12(9), 1996.

Vizcaino Naranjo, F., Acosta Espinoza, J. L., & Machuca Vivar, S. (2023). Exploring the Fusion of Blockchain and AI for Enhanced Practices in IoT Ecosystems: Opportunities and Challenges. Fusion: Practice & Applications, 13(2).

Weiquan Ni, Xumin Huang, Junxing Zhang, and Rong Yu. Healchain: (2019). A decentralized data management system for mobile healthcare using consortium blockchain. In 2019 Chinese Control Conference (CCC), pages 6333–6338. IEEE.

Wen, F., Yang, L., Cai, W. and Zhou, P., (2020). DP-Hybrid: a two-layer consensus protocol for high scalability in permissioned blockchain. In Blockchain and Trustworthy Systems: Second International Conference, BlockSys 2020, Dali, China, August 6–7, 2020, Revised Selected Papers 2 (pp. 57-71). Springer Singapore.

Williams, L. J., Hartman, N., and Cavazotte, F. (2010). Method variance and marker variables: A review and comprehensive CFA marker technique. Organizational research methods, 13(3), 477-514.

Wilson, V. (2014). Research Methods: Triangulation. Evidence Based Library and Information Practice, 9(1), 74–75.

Wong, C. S., & Law, K. S. (2002). The Effects of Leader and Follower Emotional Intelligence on Performance and Attitude: An Exploratory Study. The Leadership Qartly, 13, 243-274.

Xiaoyang Zhu and Youakim Badr. (2019). Fog computing security architecture for the internet of things using blockchain-based social networks. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pages 1361–1366. IEEE.

Xie, H., Zheng, J., He, T., Wei, S., & Hu, C. (2023). TEBDS: A Trusted Execution Environment-and-Blockchain-supported IoT data sharing system. Future Generation Computer Systems, 140, 321-330.

Xuan, S.; Zhang, Y.; Tang, H.; Chung, I.; Wang, W.; Yang, W. (2019). Hierarchically Authorized Transactions for Massive Internet-of-Things Data Sharing Based on Multilayer Blockchain. Appl. Sci. 9, 5159.

Xue, H., Chen, D., Zhang, N., Dai, H. N., & Yu, K. (2023). Integration of blockchain and edge computing in internet of things: A survey. Future Generation Computer Systems, 144, 307-326.

Xueping Liang, Juan Zhao, Sachin Shetty, Jihong Liu, and Danyi Li. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pages 1–5. IEEE.

Yadav, A. M., & Sharma, S. C. (2023). Cooperative task scheduling secured with blockchain in sustainable mobile edge computing. Sustainable Computing: Informatics and Systems, 37, 100843.

Yamane, T. (1967). Statistics, an introductory Analysis 2nd Edition: Horper and Row. New York.

Yaqoob, I., Salah, K., Jayaraman, R. and Al-Hammadi, Y., (2021). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, pp.1-16.

Yeboah-Ofori, A., Sadat, S. K., & Darvishi, I. (2023). Blockchain Security Encryption to Preserve Data Privacy and Integrity in Cloud Environment. In 2023 10th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 344-351). IEEE.

Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. (2014). Internet of Things for Smart Cities. IEEE Internet Things J., 1, 22–32.

Zehui Xiong, Yang Zhang, Dusit Niyato, Ping Wang, and Zhu Han. (2018). When mobile blockchain meets edge computing. IEEE Communications Magazine, 56(8):33–39.

Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2010). Business research methods. Mason: South Western Cengage Learning.

Zikmund, W.G. (2003). Business Research Methods. 7th Edition, Thomson/ South-Western.

Zubaydi, H. D., Varga, P., & Molnár, S. (2023). Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. Sensors, 23(2), 788.

Zulhuda, S. and A. Sayuti, (2017). Whither Policing Cryptocurrency in Malaysia? IIUM Law Journal, vol. 25 (2), pp. 179-196.

APPENDICES

Appendix A

Research Questionnaire

DATA MANAGEMENT IN THE INTERNET OF THINGS VIA EDGE COMPUTING USING BLOCKCHAIN TECHNOLOGY

Dear Sir/Madam,

My name is Edidiong Bassey Bassey and I am currently pursuing my Master's degree in Computer Science in Universiti Putra Malaysia. As part of my course, I am required to complete a research study and my chosen topic is "Data Management in the Internet of Things via Edge Computing using Blockchain Technology".

I have chosen this topic due to the increased need for improvement of data management, security and privacy of participating nodes in a big network. Based on the analysis concluded in this study, new approaches and suggestions in enhancing data management, security and privacy will be proposed.

I greatly appreciate your assistance in filling in your best honest answer, and I would like to assure you that all information shared is kept confidential and only for academic purposes.

Thank you for your precious time and participation in this study.

Kind Regards,
Edidiong Bassey

Section A: Personal Background

Please tick the most appropriate answer for each question

1. Age Group

- [ ] 25 years old and below
- [ ] 26 – 35 years old
- [ ] 36 – 45 years old
- [ ] Above 46 years old

2. Gender

- [ ] Male
- [ ] Female

3. Work Positions

- [ ] Lower Employee [supervisors, workers, and foremen].
- [ ] Middle Management [general managers, branch managers, and department managers].
- [ ] Top Management [CEO, COO, CFO, President, or Vice President].

4. Education Levels

- [ ] Diploma
- [ ] Bachelor's Degree
- [ ] Masters
- [ ] PhD

5. Tenure of Work in The Present Employment

- [ ] Less than 5 years
- [ ] 5 – 10 years
- [ ] 11- 15 years
- [ ] 16 – 20 years
- [ ] Above 20 years

6. In Which Sector is Your Firm (Select only 1 answer)

- [ ] Cloud Hosting
- [ ] Online Services and Retails
- [ ] Data Mining
- [ ] Manufacturing
- [ ] Banking and Finance
- [ ] Sports and Entertainment

☐ Education
☐ Media and Advertisement

7. Enterprise Size?

☐ Small enterprises
☐ Medium enterprises
☐ Big enterprises

SECTION B: Blockchain, Smart Contract and IoT Understanding

GENERAL DIRECTIONS

Please tick the most appropriate answer for each question

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	**2**	**3**	**4**	**5**

PART One: Your Understanding of Blockchain Technology

	Ranking	***1***	***2***	***3***	***4***	***5***
1	*Blockchain decentralised feature has no single point of failure*					
2	*Blockchain have better data security and privacy*					
3	*Blockchain provide better transparency and traceability*					
4	*Blockchain has increased efficiency and reduced costs*					
5	*Blockchain technology permits data verification without need for third-parties.*					

PART Two: Awareness Level Evaluation

1.	*Are you aware of centralised and decentralised distribution system?*					
2.	*Are you aware of blockchain, smart contracts, edge computing and iot?*					
3.	*Are you aware of blockchain use in iot?*					
4.	*Are you aware of smart contract use in iot?*					
5.	*Are you aware of blockchain use for data management?*					

PART Three: Your Opinion

1.	*Does the subject of blockchain have any role to play in data management?*					
2.	*Does blockchain have any role to play in data security and privacy?*					
3.	*Is big blockchain, smart contract and iot related to each other?*					
4.	*Blockchain is helpful in increasing IoT data security and management?*					
5.	*Will you recommend blockchain technology to management of your company?*					

PART Four: Blockchain with IoT

1.	*Does the subject of blockchain have any role to play in data management?*					
2.	*Does blockchain have any role to play in data security and privacy?*					
3.	*Is big blockchain, smart contract and iot related to each other?*					
4.	*Blockchain is helpful in increasing IoT data security and management?*					
5.	*Will you recommend blockchain technology to management of your company?*					

Appendix B

Factor Analysis

Williams et al. (2010) assert that factor analysis is a robust methodology employed in the development, enhancement, and evaluation of tests, scales, and measurements. According to Pallant and Tennant (2007), factor analysis is utilised in research to extract factors from the data and assess the suitability and appropriateness of each item for factor loading. Factor analysis can be categorised into two main components, namely Confirmatory Factor Analysis (CFA) and Exploratory Factor Analysis (EFA) (Tabachnick and Fidell, 2007). The use of CFA provides a means to assess the validity of measurements and offers an accurate technique for evaluating dimensionality, as outlined by Anderson and Gerbing (1988). On the other hand, EFA is an empirical methodology that may be employed to achieve data summarization and data reduction, as discussed by Hair et al. (2014). In addition, Harris and Brown (2010) asserted that CFA differs from EFA in that it is guided by predetermined models and theories on the number of constructs, and expects the constructs to align with these models or theories. Hence, in this work, the exploratory factor analysis (EFA) was utilised as the primary method to identify the underlying latent dimension represented by the original data.

Exploratory Factor Analysis

The utilisation of EFA facilitates the extraction of the maximum amount of variance from a given dataset. This process ensures that the initial component captures the most variance, while the final component captures the least variance (Tabachnick and Fidell, 2007). EFA was performed in order to examine the underlying structure of the measurement items that align with the components outlined in the conceptual framework. Principal component analysis (PCA) was selected as the primary method for executing the initial solutions for the EFA from a range of extraction techniques (Tabachnick and Fidell, 2007). Moreover, PCA aids in the identification and reduction of a vast array of variables by transforming correlated variables into new independent linear composite variables (Hair et al., 2014). The researchers opted for the utilisation of the orthogonal varimax rotational technique for the purpose of extraction. The orthogonal varimax approach is frequently employed and is known for its superior replicability and generalizability when compared to the oblique rotational method (Pallant, 2007).

According to the findings of Rennie (1997), the application of orthogonal rotations yielded results that exhibited optimal fit with both historical and prospective data. The results obtained from the oblique rotation demonstrate the highest level of congruence with the data gathered in the present survey investigation. Moreover, the interpretation of data produced through orthogonal rotation is facilitated by the absence of correlations between variables, as compared to the oblique method (Tabachnick and Fidell, 2007; Pallant, 2007). Three criteria were chosen to evaluate the appropriateness of the extracted factors: the percentage of variance criterion, the scree test criterion, and the latent root criterion. According to Hair et al. (2014), eigenvalues that are bigger than one adheres to the latent root criterion. Additionally, a solution that encompasses 60% or more cumulative variance fulfils the requirement of variance percentage. Hair et al. (2014) further suggest that the commonality of an original variable refers to the total variance it shares with other variables.

According to Field (2006), an item that exhibits no variance is characterised by a commonality value of (1). Similarly, a variable that does not share any similarities with other variables is associated with a commonality value of zero (0). According to Hair et al. (2014), items with a commonality below 0.5 (50%) are classified as weak items. According to Pallant (2007), it is advisable to accept a cut-off value of communality if the sample size is 0.3. In order to get favourable results in factor analysis, it is recommended to assess the appropriateness of sampling through the utilisation of the Kaiser-Meyer-Olkin (KMO) test, as well as to evaluate the sphericity of the data using Bartlett's test (Norusis, 1992). KMO value greater than 0.6 indicates a statistically significant association between items and is considered appropriate for doing EFA in order to obtain a concise collection of components. On the other hand, the Bartlett's test of sphericity suggests that the correlation between the measurement items exceeds 0.3, therefore making it appropriate for EFA (Hair et al., 2014).

In the present study, the inherent data was utilised to conduct EFA on four distinct sets of items collected from the fields of usefulness, awareness, and adoptability rate of Blockchain with IoT ecosystem literature. The 20 questions response underwent EFA in order to contribute to the development of four constructs that have been developed in theory. The present study conducted the EFA test in accordance with Byrne's (2010) advice. The findings indicated that the Kaiser-Meyer-Olkin (KMO) value of 0.931 exceeded the minimum threshold of 0.6, demonstrating adequate sampling adequacy for conducting EFA. Additionally, Bartlett's test yielded a significant result ($p < 0.005$), further supporting the suitability of the data for EFA. These results are summarised in Table 1. (Kaiser, 1974; Bartlett, 1954) have been cited in the literature.

Table 1 : Kaiser-Meyer-Olkin Test Result

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.931
Bartlett's Test of Sphericity	Approx. Chi-Square	5251.910
	df	190
	Sig.	.000

Table 2 presents the commonality of individual items. All products have component similarities that are higher than the average 0.5 (.500). In order to enhance or optimise the scale, it is necessary to eliminate elements with low commonality, as suggested by Hair (2014).

Table 2 : Communalities Extracted

	Initial	Extraction
PSD1	1.000	.686
PSD2	1.000	.669
PSD3	1.000	.649
PSD4	1.000	.763
PSD5	1.000	.718
PSA1	1.000	.640
PSA2	1.000	.734
PSA3	1.000	.715
PSA4	1.000	.737
PSA5	1.000	.662
PSM1	1.000	.679
PSM2	1.000	.778
PSM3	1.000	.813
PSM4	1.000	.786
PSM5	1.000	.748
BIE1	1.000	.755
BIE2	1.000	.765
BIE3	1.000	.643
BIE4	1.000	.801
BIE5	1.000	.751

Extraction Method: Principal Component Analysis.

Table 3 presents the comprehensive variation accounted for by each component. Table 3 presents the initial four (4) component outcomes the components exhibited eigenvalues greater than one. The cumulative percentage in the column indicates that the four components accounted for a total variance of 72.453%, surpassing the recommended threshold of 60%. The significance of the number of components that contributed to an eigenvalue greater than one was acknowledged, while the remaining factors were deemed insignificant and thereafter disregarded (Hair et al., 2014).

Table 3 : Total Variance Explained by Each Component

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	10.169	50.846	50.846	10.169	50.846	50.846	3.833	19.164	19.164
2	1.755	8.775	59.622	1.755	8.775	59.622	3.667	18.335	37.499
3	1.441	7.205	66.827	1.441	7.205	66.827	3.552	17.760	55.259
4	1.125	5.626	72.453	1.125	5.626	72.453	3.439	17.194	72.453

Extraction Method: Principal Component Analysis.

According to existing literature, it has been observed that factors extracted using Kaiser's criterion alone, namely those with eigenvalues greater than 1, tend to result in an overestimation of the number of components removed (Hubbard and Allen, 1987). To validate the factors identified using Kaiser's criterion, an additional statistical technique known as Horn's parallel analysis (Horn, 1965) was employed. The Monte Carlo Principal Component Analysis (PCA) application was utilised to conduct simulations on a dataset consisting of 349 samples and 20 predicted items. This process generated 349 supplementary random datasets. The eigenvalues produced via the SPSS data reduction approach were compared with the eigenvalues acquired from the random data set utilising parallel analysis. Table 5 presents the results indicating that for components 1 to 4, the eigenvalue derived from principal component analysis (PCA) did exceed the criteria value obtained from the parallel analysis (i.e., 10.169 > .203507). Hence, a total of five components were selected for retention, while the remaining components were deemed unsuitable and excluded from the analysis (Pallant, 2007).

Table 4 : Parallel analysis for confirming the factors extracted using PCA

Component	Actual Eigenvalues from PCA	Criterion Values from Parallel Analysis	Decision
1	10.169	.203507	Accept
2	1.755	.079627	Accept
3	1.441	-.000454	Accept
4	1.125	-.061894	Accept

Additionally, the scree test served as the third criterion in the determination of the number of components. The scree test is a method used to visually represent the relationship between the latent roots and the number of components in their extraction sequence. By examining the form of the curve inside the plot, researchers can decide the appropriate cut-off point (Hair et al., 2014).

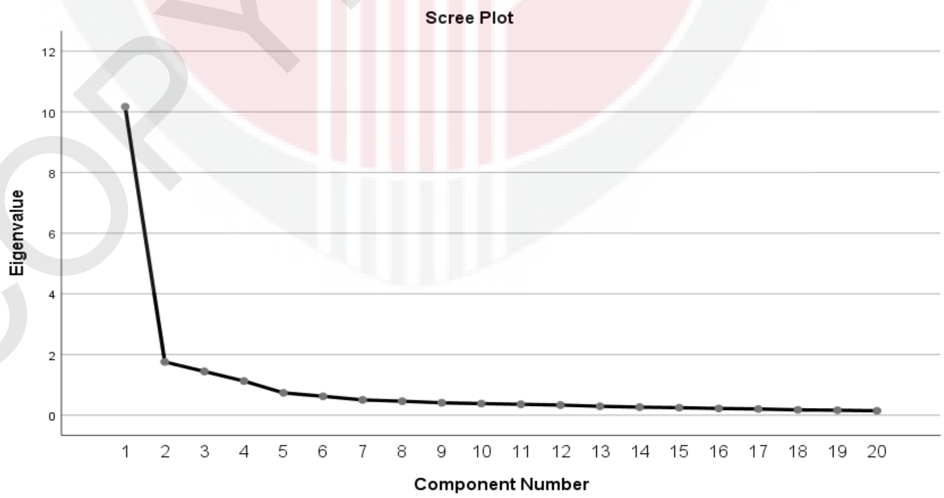

Figure 1 : Scree Plot of All the Dimensions

According to Tabachnick and Fidell (2007), the plot's form exhibits a decreasing trend as it progresses from the factor with the highest eigenvalue to the factor with the lowest eigenvalue, ultimately culminating in the final factor with the lowest eigenvalue. The observed alteration in the configuration of the graph, typically taking the form of an elbow, serves as a discernible indication of the evident differentiation between components of significance possessing eigenvalues greater than one, and those that are disregarded due to their eigenvalues being less than one (Hair et al., 2014). The present study includes an examination of the scree plot (Figure 4.8), which serves to validate the extraction of a comparable number of components based on Kaiser's latent root criterion, specifically, eigenvalue greater than one. The graph exhibited a distinct delineation between the components. Components 1 to 4 exhibited a higher degree of variance explanation or capture compared to the remaining components.

Table 6 : Pattern Matrix (Rotated)

	Component			
	1	2	3	4
PSD1				.747
PSD2				.716
PSD3				.697
PSD4				.758
PSD5				.718
PSA1			.701	
PSA2			.765	
PSA3			.761	
PSA4			.748	
PSA5			.716	
PSM1		.721		
PSM2		.746		
PSM3		.805		
PSM4		.772		
PSM5		.789		
BIE1	.782			
BIE2	.786			
BIE3	.711			
BIE4	.829			
BIE5	.759			

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalisation.
a. Rotation converged in 6 iterations.

The rotating pattern matrix in Table 6 ultimately revealed 4-factor solutions. It is recommended that there be a strong connection, with a factor loading higher than 0.6, between the concept and its measuring item (Henseler et al., 2009). Furthermore, certain experts in psychometrics (Churchill, 1979) propose the removal of items that exhibit a factor loading below 0.4. The pattern matrix table displays the outcomes indicating that the items were loaded onto four factors, with factor loadings ranging from 0.697 to 0.829. These loadings meet the minimum criterion for factor loading as outlined by Churchill (1979), Pallant (2007), and Hair et al. (2014). After the extraction of factors, it becomes necessary to determine the number of things that are loaded onto each respective component using the consistency analysis. The consistency of each component with relevant items is assessed using Cronbach's alpha measure (Cronbach, 1951).

BIODATA OF STUDENT

Edidiong Bassey Bassey was born on 19 November 1988 in Uyo, Akwa Ibom State Nigeria. He received his early education at St. Christopher's Nursery and Primary school, Calabar. He moved on to Hillside International School, Uyo where he completed his primary education. He continued his education at NCI, Uyo where he finished his Secondary Education. He received a Bachelor's degree in Software Engineering from the Univeristy of East London. He is currently a research student of Universiti Putra Malaysia, Faculty of Computer Science and Information Technology. His current research work is on DATA MANAGEMENT MODEL FOR INTERNET OF THINGS DEVICES IN EDGE COMPUTING ENVIRONMENT USING BLOCKCHAIN TECHNOLOGY.