
# Blockchain Framework for Enhancing Employment Integrity Process to Curb Ghost Worker Fraud

Musa Ibrahim Bello

Cybersecurity Research Group

Department of Computer and Information Sciences

University of Strathclyde, Glasgow

February 25, 2026

A thesis submitted for the Degree of Doctor of Philosophy

# Declaration

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree.



Signed:

Date:

# Abstract

Ghost worker fraud, where fictitious employees are inserted into payroll systems to divert public funds remains a pervasive and costly challenge in Nigeria's public sector. Although the Integrated Payroll and Personnel Information System (IPPIS) was introduced to improve accountability and transparency, recent literature and empirical evidence continue to show that the system has not effectively mitigated fraudulent employment practices. This research addresses these shortcomings by developing the Decentralized Employment Integrity and Fraud Prevention (DEIFP) framework, a blockchain-based model designed to strengthen integrity, verification, and auditability across the public sector employment lifecycle. The study employs a mixed-methods strategy, combining two independent survey studies conducted in 2021 and 2024 with qualitative case analysis of high-profile employment fraud incidents. The empirical findings reveal that government employees consistently perceive IPPIS as susceptible to insider manipulation, and weak verification controls. Evaluations from blockchain experts further highlight the need for decentralised trust infrastructures that can provide tamper-resistant validation and transparent recordkeeping in multi-agency employment contexts. Drawing on the principles underlying consortium blockchains and the security offered by Ethereum Besu, the proposed DEIFP framework is conceptually designed to enable decentralised validation of employment records. Rather than replacing existing systems, it re-architects the trust model by distributing validation responsibilities across authorised government institutions, thereby reducing reliance on a single point of failure and limiting opportunities for the insertion of ghost workers. This thesis contributes a conceptual design of the DEIFP framework, introducing a novel blockchain-based model for decentralised employment validation in the public sector. It also integrates insights from information systems, fraud theory, and governance to establish an interdisciplinary foundation for technology-enabled fraud prevention. Lastly, the study recommends piloting the framework in real operational environments and emphasises the need for strong policy and regulatory alignment to support trust, compliance, and future adoption in Nigeria's public sector.

# Contents

# List of Figures

List of Figures

# List of Tables

# Acknowledgements

In the name of Allah, the Most Gracious, the Most Merciful. First and foremost, I extend my deepest gratitude to Allah for granting me the strength, patience, and wisdom to embark on and complete this challenging journey. Secondly, I would like to express my sincere gratitude and appreciation to my supervisor, Dr. Daniel Thomas for his invaluable guidance, support, and encouragement throughout the course of this research. His expertise, kindness and constructive feedback were instrumental in shaping this work, and I am deeply grateful for his mentorship. Many thanks to my second supervisor Dr. Sotirios Terzis for his contribution to the success of this work. I am deeply indebted to my parents, Alhaji Ibrahim Bello and Hajiya Ummul Kulshumi Umar, whose prayers, love, and encouragement have been the foundation upon which all my achievements rest. I am immensely thankful to the Petroleum Technology Development Fund (PTDF) for providing the financial support necessary to pursue this research. Their funding and commitment to education and research have been pivotal in making this work a reality. To my beloved wife, Ummulkhair Hassan, thank you for your unwavering love, patience, and understanding. You have been my pillar of strength, especially during the challenging times. I also dedicate this work to my precious daughter, Ummulkulshumi (Deenat) who was born during this journey. Your presence brought immense joy and motivation to see this project through to completion. I extend my gratitude to my dear friends who dedicated their time and effort to proofread and provide valuable feedback on my work. Your friendship, support, and encouragement have been invaluable, and I am forever thankful. Finally, to all who have contributed in one way or another to the completion of this thesis, I express my heartfelt thanks. Your support has been a source of great strength and inspiration.

**“Say, “Are those who know equal to those who do not know?’ Only those who are endowed with understanding will take heed.” - Holy Qur’an (39:9)**

# Publications and activities

The following are the peer-reviewed publications resulting from the research described within this dissertation:

1. Bello, M. I., & Thomas, D. R. (2025). Blockchain framework for enhancing employment integrity process to curb ghost worker fraud: NCSC ACE-CSR Conference 2025.

   The poster contained extracts from Chapter 1, subsection 6.4.1 and images from subsection 6.4.2 and Figure 6.2

2. Bello, M. I., & Thomas, D. R. (2023). Curbing ghost worker fraud in developing countries using consortium blockchain. *Proceedings of the 9th ACM International Workshop on Security and Privacy Analytics*, 77–83. https://doi.org/10.1145/3579987.3586569

   The paper contained extracts from Chapter 1, Chapter 2 and images from Figure 2.3 and Figure 5.1. The paper examined the problems of IPPIS. We then propose the use of a consortium blockchain framework to tackle ghost worker fraud and detail the type of consensus algorithm and the blockchain structure required. The paper was peer reviewed.

3. Bello, M. I., & Thomas, D. R. (2022). Potentials of blockchain technology for payroll systems. *SAIS 2022 Proceedings*. https://aisel.aisnet.org/sais2022/20/

   The paper contained extracts from some parts of Chapter 1 and some parts of Chapter 2. The paper examines the problems of payroll systems in developing countries and how the capabilities of blockchain could be harnessed to solve them. The paper was peer reviewed.

4. Bello, M. I. (2021a). Blockchain Technology and Payroll Systems. https://pureportal.strath.ac.uk/en/activities/improving-payroll-systems-in-developing-

countries-using-blockchai%20University%20of%20Strathclyde,%20Glasgow%20-%20United%20Kingdom

This was the conceptual view of my early work which was obtained from some part of Chapter 1 of the thesis.

## Paper under development

Bello, M. I. & Daniel R. Thomas, Design of Decentralized Employment Integrity and Fraud Prevention Framework (DEIFP) To Curb Ghost Worker Fraud This paper will be culled from excerpts from Chapter 1, Chapter 2, Chapter 6 and Chapter 4. The key contributions of the paper are: Increasing the understanding and application of blockchain technology within the governance sector, particularly in the areas of transparency and fraud prevention. Assessing the perceptions of government employees and blockchain experts regarding the factors influencing ghost worker fraud in Nigeria, and proposing a solution. Ultimately, mixed method approach will be applied, giving the framework robust evaluation and assessment. I intend to send this paper to the IEEE Computer Society for publication under the IEEE Transactions on Dependable and Secure Computing.

## Academic citizenship

1. Bello, M. I. (2022). Doctoral School Multidisciplinary Symposium 2022 - University of Strathclyde. https://pureportal.strath.ac.uk/en/activities/strathclyde-doctoral-school-multidisciplinary-symposium-2022-even

   This was a peer review abstract I conducted in 2022 during the annual DSMS.

2. Bello, M. I. (2021b). Doctoral School Multidisciplinary Symposium 2021 - University of Strathclyde. https://pureportal.strath.ac.uk/en/activities/doctoral-school-multidisciplinary-symposium-2021-event-3

   This was a peer review abstract I conducted in 2021 during the annual DSMS.

3. Bello, M. I. (2021c). The Scottish Informatics and Computer Science Alliance (SICSA) (External organisation). https://pureportal.strath.ac.uk/en/activities/the-scottish-informatics-and-computer-science-alliance-sicsa-exte I was a member of the SICSA Conference Advisory Board during the 2021 conference. We plan, organize, and assisted in conducting the conference.

# Chapter 1

# Introduction

Employment fraud is a common financial problem for governments and organizations across the world. This is because of inefficient and ineffective management as well as weak internal controls [351]. These frauds have alarming consequences in all nations, contributing to untold suffering and increase of unemployment [320]. Fraud is not a new phenomenon, it has long been a persistent issue in organizations and public sectors [339]. In Nigeria today, fraud has become a norm in all aspects of life. It belongs to the many different categories of corruption [3]. Fraud in many instances especially financial crimes in Nigeria occur as a result of economic hardship and the pressure to get rid of poverty [271].

One critical form of fraud in organizations is ghost worker fraud. A ghost worker is any individual who is included fraudulently in a company or government's payroll system and receives salary but does not do any work. Individuals who receive salaries and other benefits in place of a dead, resigned, or retired employees are also ghost workers [271]. The public sector in Nigeria is burdened with ghost workers, these people do not present themselves for job interviews nor write job applications, but still open bank accounts and receive monthly salaries [223]. In Nigeria, billions of Naira (millions of GBP) are defrauded due to ghost worker fraud [247], this led to major drawbacks to the economy [271].

Regardless of the payroll system architecture, it is personnel in strategic locations who add new employees, some of whom may be ghost workers [420]. The ghost worker issue is connected to non-transparent and poor payroll and employment process management, as highlighted in Chapter 4 and Chapter 8. Payroll and employment processes need to be enhanced to deal with the problem of ghost workers [358]. To tackle the menace of ghost worker fraud in Nigeria, different administrations have introduced

different measures and strategies.

One of the numerous solutions employed to curb ghost worker fraud is the deployment of the IPPIS in 2006 as detailed in section 2.6 and later the Government Integrated Financial Management Information system (GIFMIS) in 2012 [144]. IPPIS is an integrated platform the government use for payroll, and employment purposes. One of the cardinal objectives of the previous government, (Government of President Buhari 2015 to 2023) was to fight corruption. His government implemented and enforced Treasury Single Account (TSA), E-Payment, and IPPIS among others to tackle financial corruption and other related frauds. Treasury Single Account (TSA) is a public accounting system in which all government revenue, receipts, and income are collected into a single account, which is normally handled by the nation's central bank. The primary goal is to reduce corruption, ensure efficient cash management, eliminate idle funds, and improve tax collection and payment reconciliation [23].

However, reports and empirical studies indicate that there are still issues with the existing system. For example, Onukelobi et al. analyzed IPPIS and GIFMIS and found that both failed to stop ghost worker fraud [294]. In 2022, the Federal Government detected 1,500 ghost workers in its payroll and suspended 3,000 employees who refused to come for verification [436]. Therefore, this thesis is motivated by the substantial financial losses and inefficiencies resulting from ghost worker fraud in the employment process. This fraudulent activity undermines public trust and depletes resources that are intended for legitimate employees and other public projects. The problem statement emphasizes the difficulties presented by the IPPIS, which, despite achieving its objectives, has not fully resolved the problem.

In this chapter, research objectives and research questions that guide the study to creating a secure and transparent solution using blockchain technology, specifically Ethereum Besu were outlined. This chapter also presents a review of the IPPIS, including its role, functionality, and the underlying issues that require more investigation. It highlights the significance of using a blockchain-based approach to transform the employment process ensuring transparency were presented. Lastly, the chapter ends by providing a summary of the structure of the thesis and explaining how each subsequent

chapter plays a role in achieving the research objective.

Furthermore, the initial publication titled "Potentials of Blockchain Technology for Payroll Systems" [55] incorporated elements from this section, particularly the discussion on how blockchain can improve payroll systems. These insights formed the foundation for assessing blockchain's potential to resolve issues of integrity and transparency within Nigeria's public sector payroll. In the second paper "Curbing Ghost Worker Fraud In Developing Countries Using Consortium Blockchain" [56], the role of blockchain technology in addressing ghost worker fraud in developing countries was discussed .

## 1.1 Who are the ghost workers

Nafiu et al. identified ghost workers in different types based on situation and cause [271]:

**Fictitious employee:** This is when a timesheet is altered by a supervisor or someone with great influence and salary is diverted to a false bank account. It is the most widespread scheme and the easiest to detect.

**Pre-employment ghost employee scheme:** This type of ghost worker is created before a legitimate employee begins work. It involves a salary going to someone's account in the name of the employee who is yet to begin working.

**No-show ghost employee scheme:** when a legitimate employee does not show up and the supervisor enters into a deal with the employee to enjoy a percentage of the employee's salary.

**Family members as ghost employees:** this is one of the most common types of ghost workers. When a family member's name (such as a minor) is captured on a payroll and payment is made into a false bank account.

**Unclaimed payroll cheque scheme:** when an employee is relieved from a position (usually a top position) without formal procedures and his/her details and status

remains intact. Some top officers claim some payments.

**Termination ghost employee scheme:** when an employee is sacked or retires without due process, it allows ghost worker fraud, where some staff will fraudulently claim their salaries and other entitlements. Ghost workers do not evolve on their own, they must be hired, created, and encouraged by other individuals [271].

According to Hawley, the people at the helm of affairs are usually involved in ghost worker fraud scheme, either knowingly or unknowingly [168]. For every ghost worker to exist, they must be hired, there must be likely some authorization for every periodic payment, and ghost workers must need to somehow access their payment. Despite the architecture of the payroll system and employment process, the people in strategic places are the ones who add new employees, which could be ghost workers [420]. The majority of the literature agrees on the need to enhance data systems to deal with the problem of ghost workers [358]. Hussmann asserts that ghost workers could be reduced by ensuring better transparency in recruitment and promotion processes [181].

The Nigerian government implemented the Integrated Personnel and Payroll Information System (IPPIS) as a way to improve the payroll management and employment process of the federal civil service by increasing transparency, accountability, and efficiency. Despite the implementation, the ghost worker issue has not been totally resolved. The system is still being exploited by fraudsters, who fabricate bogus employee records and steal public funds covertly. Hence, the need to combat ghost worker fraud in Nigeria and improve the reliability of the public payroll system is what motivated this study. Therefore, this study proposed the use of blockchain technology, in particular the Ethereum Besu platform, as a cutting-edge fix to this ongoing issue. Blockchain technology offers special qualities like immutability, transparency, and decentralization that could be used to build a secure and tamper-proof employee data ledger, making it much more difficult for fraudsters to add ghost workers into the system while making employment process seamless.

## 1.2 Problem statement

The Nigerian Government is currently using the IPPIS for payroll platform and employment purposes [406]. Aluko stated that among IPPIS's numerous issues is ghost worker fraud through employment process [24]. The smuggling of ghost workers in a payroll system is a fraudulent act, along with the theft of government money and kickbacks [289]. After thorough and methodical screening, 84 000 ghost workers were eliminated from the Nigerian government payroll system between 2014 and 2016 [247]. In 2021, the government of Borno State found that it had 22 556 ghost workers that cost it 420 million Naira (almost half a million GBP) per month (The Ghost Workers Syndrome in Nigeria, 2021). Furthermore, in 2016 the Nigerian Federal Government found an estimated 65K ghost workers in the IPPIS [331].

Ghost worker fraud is not only a Nigerian problem, but also a global problem, which accounts for a significant percentage of public employees [252] for example, in the United States of America, a former assistant controller embezzled hospitals' funds through forgery and alteration of the payroll system. Termination pay was paid to sacked employees and deposited in accounts operated by the Assistant Controller (United States Department of Justice, 2015). Similarly, a health claim director in the United States was convicted of embezzling US$846 000 through a ghost worker scheme [81].

In 2014, 30.6 percent of the total Yemeni labor force was in the government payroll system, a significant number of them were ghost workers who did not exist, but collected salaries. This was a serious concern for the Yemeni government as they have limited resources to cope with thousands of unemployed people [15]. Similarly, in Uganda, some health workers falsify documents to create false health centers only to steal funds allocated to the ghost workers [270]. In addition, in Afghanistan, ghost workers were reported to have infiltrated the government's payroll system. The United States government was concerned that funds that were meant to pay Afghan police salaries were going to ghost workers. The European Union one time withheld 100 million Euros meant to contribute to the Afghan Trust Fund due to the possibility of not using the money for the real workers [377]. According to Shin, there are two types of payroll

fraud; timecard falsification and ghost worker fraud. They termed the latter as the most common [365].

Despite the implementation of IPPIS, ghost worker fraud remains a significant challenge within Nigeria's public sector. Numerous instances of ghost worker fraud across different levels of government highlight the critical flaws in the existing payroll and employment management process. For example, the Anthony Ogar case in 2020 defrauded the Nigerian government of ₦140 million (74 000 GBP) by fabricating ghost worker records [396], and the Dairo Samson case in 2017 similarly defrauded the government of ₦11.3 million (6 000 GBP) [125]. Also, in other climes there are cases of Dr. Mzalendo Kibunja and his accomplices who defrauded the National Museums of Kenya by creating and paying ghost workers the sum of Kes 449 392 075 (approximately 2 900 000 million GBP). More so, there is the Leicestershire case [46], where a group of fraudsters scammed a cancer charity and the local council of thousands of pounds. These cases emphasize the systemic failure to detect and prevent fraud.

The persistence of ghost worker fraud highlights the need for a more secure and transparent solution to address these vulnerabilities in the system. Blockchain's immutable and decentralized nature could offer a more robust and tamper-proof mechanism for employment management, where multiple independent agencies could verify employment records and validate the authenticity of the personnel data [358]. In conclusion, the continued prevalence of ghost worker fraud despite the introduction of IPPIS necessitates a reevaluation of the system and the implementation of a more transparent and effective solution. The current vulnerabilities in the payroll and employment system are not unique to Nigeria, but are found in various public sector systems around the world. A decentralized blockchain-based framework, such as the one proposed in this research, could address these vulnerabilities by enhancing transparency, security, and accountability within the employment verification process.

## 1.3 Research aim and objectives

The aim of this research is to propose a blockchain framework that could improve transparency and data integrity within the employment process to curb ghost worker fraud in Nigeria by integrating blockchain technology and some external organizations with the existing IPPIS.

### 1.3.1 Research objectives

The primary objectives of this research are as follows:

1. Understand Government Employee Perceptions: To investigate how government workers feel about the employment process via the IPPIS and its probable connection to ghost worker fraud.

   Because by understanding how government employees perceive the IPPIS, one can gauge the system's effectiveness in addressing ghost worker fraud. If employees feel the system is inadequate, it points to the gaps that need to be addressed, which is crucial to developing more effective solutions.

2. Make systematic analysis on fraud theoretical frameworks: This will help identify the most relevant theoretical frameworks for understanding ghost worker fraud, ensuring that the study is grounded in well-established concepts.

   Because by systematically analyzing these frameworks, it could effectively guide the development of a solution to address the specific issues of fraud.

3. To Develop a Blockchain-Base: This is a blockchain framework based on Ethereum Besu to improve the IPPIS employment process and so enhance employment integrity and effectively mitigate ghost worker fraud within Nigeria's public service.

   This is important because it proposes a solution to the issue of ghost worker fraud by leveraging blockchain technology to enhance transparency in the employment process. The development could provide a technological approach to addressing the inefficiencies in the existing system, ensuring a more trustworthy public service employment process.

4. To Define Stakeholder Roles and Responsibilities: Specify the roles of various stakeholders such as the employers, employees, validators, security agencies, and regulatory bodies in implementing and sustaining the blockchain-based framework.

   This is important because clearly defining the roles and responsibilities of various stakeholders ensures effective collaboration and accountability in the proposed framework.

5. To Evaluate the Impact of the proposed Framework through Case Study Analysis: Conducting a thorough analysis of real-world ghost worker fraud cases to assess the potential effectiveness and applicability of the framework in mitigating fraud risks and enhancing transparency in government employment systems.

   This objective is important because evaluating the proposed framework through real-world case studies allows for a practical assessment of its effectiveness in addressing ghost worker fraud. By analyzing actual fraud cases, the research could demonstrate the framework's potential impact on improving transparency and reducing fraud in government employment systems.

6. To Assess the Effectiveness of the Proposed Framework: Conducting and administering surveys to federal government employees and blockchain experts to assess the perceived effectiveness of the proposed framework.

   This objective is important because it allows for the collection of valuable feedback from key stakeholders, including government employees and blockchain experts, to gauge the perceived effectiveness of the proposed framework. By assessing their views, the research could validate the framework's feasibility, ensuring that it is both practical and acceptable to those involved in the implementation and use of the system.

### 1.3.2 Research questions

The research questions that guide this study are as follows:

1. To what extent do government employees perceive that the employment process through IPPIS encourages or facilitates ghost worker fraud?
2. What is the most appropriate theoretical framework for analysing ghost worker fraud within public sector employement process, and how can it inform the development of a blockchain-based fraud prevention framework?
3. How can a decentralized blockchain-based framework, utilizing Ethereum Besu, be designed to enhance employment integrity and mitigate ghost worker fraud within the Nigerian public service, particularly through the IPPIS employment process?
4. What are the specific roles and responsibilities of key stakeholders, including employers, employees, validaters, security agencies, and regulatory bodies, in the acceptance of the proposed framework?
5. How effective is the proposed framework in addressing the vulnerabilities and fraud risks identified in real-world ghost worker fraud cases within government employment systems?
6. How effective is the proposed framework perceived to be by government employees and blockchain experts?

## 1.4 Research scope

The case study of this research is the employment process through the IPPIS of the Nigerian government. The IPPIS is a computerized Human Resource Management Information and Payroll System that is being implemented in all Ministries, Departments, and Agencies (MDAs) to perform various human resource functions. The study will cover only the employment process through the IPPIS existing on the IPPIS platform and the attempt prevent ghost worker fraud within it. The study will not cover other functionalities of the IPPIS, such as how salaries are computed, who or when to employ, who controls the payroll, increment or decrement of salaries, and who gets promoted, demoted, or sacked.

## 1.5 Summary of Contributions

This research contributes to the fields of fraud prevention, blockchain applications, and public sector governance, with a specific focus on addressing ghost worker fraud in Nigeria. The contributions are centred on the conceptualisation of a novel blockchain-based framework, its architectural design, and its empirical evaluation through stakeholder engagement and case analysis. The key contributions are as follows:

1. Design of the DEIFP Framework: The primary contribution of this study is the design of the Decentralized Employment Integrity and Fraud Prevention (DEIFP) framework. This framework proposes a blockchain-based approach to enhancing transparency, data integrity, and fraud prevention in public sector employment systems. While a full technical implementation or proof of concept has not yet been developed, the research presents a detailed architectural design and implementation strategy. These are discussed in section 6.5, with stakeholder feedback and evaluation results presented in Chapter 7 and Chapter 8.

2. Blockchain-Driven Framework for Public Sector Employment Verification: This study introduces a novel application of blockchain technology—specifically Ethereum Besu—for decentralised validation of employment records. While blockchain has been widely explored in financial systems, its application in public sector employment verification remains under-researched. This research demonstrates how Ethereum Besu can be leveraged to enable multi-agency validation, reduce single points of failure, and enhance auditability. Technical considerations and the rationale for selecting Ethereum Besu are detailed in Chapter 5 and Chapter 6.

3. Advancing Blockchain Adoption in Public Governance: This research contributes to the growing discourse on blockchain's role in public administration by demonstrating its potential to enhance transparency, accountability, and fraud prevention in employment systems. The study offers a context-specific use case that can inform broader policy and technological adoption strategies. These implications are discussed in subsection 2.8.1 and Chapter 5.

4. Interdisciplinary Integration: The research draws on insights from information systems, blockchain technology, public administration, and fraud theory to develop a comprehensive approach to employment fraud prevention. This interdisciplinary perspective strengthens the theoretical and practical relevance of the DEIFP framework, as discussed in section 6.5.

5. Potential for Broader Application: Although the DEIFP framework is designed for the Nigerian public sector, its principles are transferable to other domains requiring secure and transparent verification processes. The study outlines how similar blockchain-based frameworks could be adapted for use in supply chain management, financial services, and other sectors vulnerable to data manipulation and fraud. These broader implications are explored in subsection 2.8.1 and Chapter 6.

## 1.6 Structure of the dissertation

This dissertation is organized into ten chapters, providing a comprehensive exploration of utilizing blockchain technology, specifically Ethereum Besu, to address ghost worker fraud in Nigeria's public sector employment processes. Below is the outline of the structure and content:

**Chapter 2: Literature Review:** This chapter provides an in-depth review of existing literature related to payment and payroll systems, corrupt practices in developing countries, and the IPPIS. It also explores the current state of ghost worker fraud in Nigeria and other similar contexts, evaluating prior attempts to resolve this problem. The chapter identifies gaps in the current knowledge and positions the study within these gaps, justifying the need for a blockchain-based approach.

**Chapter 3: Theoretical Framework:** This chapter presents the theoretical frameworks underpinning the study of ghost worker fraud and the adoption of blockchain-based systems in the public sector. The frameworks are grouped into two major categories: fraud-related theories and technology adoption models. Each theory

is critically examined for its relevance, strengths, limitations, and applicability to the research problem of ghost worker fraud. Emphasis is placed on selecting the most appropriate frameworks to guide the research design, data collection, and analysis. The chapter concludes by justifying the selected frameworks and summarizing their integration into the study.

**Chapter 4: Data analysis of the 2021 survey:** This chapter presents the 2021 survey focusing on the perceptions of federal government employees concerning the IPPIS system. The chapter offers a thorough analysis and interpretation of the survey results, showing the important elements that contribute to ghost worker fraud based on employee responses.

**Chapter 5: Ethereum Besu Concept:** This chapter describes the conceptual design of the blockchain framework using Ethereum Besu. It addresses the reasoning for using Ethereum Besu, as well as the essential components of the proposed system, such as network architecture, consensus mechanisms, and smart contract integration. The chapter lays out the framework for the subsequent development phases, outlining the main concepts that will guide the design to ensure transparency, security, and efficiency in employment processes.

**Chapter 6: Design of the decentralized employment integrity and fraud prevention framework (DEIFP):** This chapter introduces the Decentralized Employment Integrity and Fraud Prevention (DEIFP) Framework designed through the use of Ethereum Besu-based blockchain technology. The chapter explained the design science approach concept which is adopted for the methodology. The section equally outlines the conceptual design of the DEIFP Framework, detailing its objectives, key components, and implementation strategy. Additionally, it would provide a clear explanation of how blockchain's key features, such as decentralization, immutability, transparency, and security, can be leveraged to reduce ghost worker fraud in Nigeria's public sector employment processes.

**Chapter 7: Evaluation by case study:** This chapter evaluates the effectiveness of the decentralized Employment and Payroll Framework (DEIFP) in tackling ghost

worker and employment fraud. The chapter highlights systemic weaknesses in payroll and employment verification processes by analysing various high-profile fraud cases. The effects of weak access control, inadequate monitoring, and lack of cross-agency verification are investigated in real-world fraud schemes. The DEIFP framework, which includes decentralized data sharing, strong verification process, stakeholder collaboration, access control and security, and feedback mechanism, is evaluated for mitigation and prevention of future fraud. The analysis shows how the DEIFP framework may improsec:2024 analysisve employment processes and detect and prevent ghost worker fraud.

**Chapter 8: Data analysis of the 2024 survey:** This chapter presents the 2024 survey which was conducted in 2024 to assess the proposed framework for Decentralized Employment Integrity and Fraud Prevention (DEIFP). The chapter offers a thorough analysis and interpretation of the survey results, showing the important elements that contribute to ghost worker fraud based on employee responses and their perceptions on the proposed DEIFP framework.

**Chapter 9: Discussion of findings:** The quantitative results of the 2021 and 2024 surveys as well as case studies on the IPPIS and the proposed DEIFP Framework are included in this chapter. The two main study themes: (1) the ineffectiveness of IPPIS in reducing ghost worker fraud and (2) the potential effectiveness of the DEIFP framework in addressing the identified systemic weaknesses. This chapter attempts to present a picture of the present situation of employment verification in the public sector, the difficulties confronting IPPIS, and the feasibility of DEIFP as a solution by assessing both the survey results and actual case studies.

**Chapter 10: Future work:** This chapter identifies potential areas for further research and development, direct extensions and new approaches, such as implementing the framework, integrating advanced analytics and machine learning, expanding the application scope to other human resource management areas, and conducting pilot studies to test the system in real-world settings.

**Chapter 11: Conclusion:** This chapter summarizes the key findings and contribu-

tions of the study, reflecting on how the research objectives were met. It provides a conclusive statement on the effectiveness of using Ethereum Besu to mitigate ghost worker fraud in Nigeria's public sector. The chapter also offers final recommendations for stakeholders and policymakers regarding the broader adoption of blockchain technology in public governance.

# Chapter 2

# Literature Review

This literature review critically analyses previous work on payroll and employment systems, corruption in developing countries, and blockchain technology. Its purpose is to identify research gaps, assess limitations of systems like IPPIS, and compare blockchain with alternative technologies (PKI, AI, RPA, etc.). The chapter synthesises interdisciplinary perspectives to justify the selection of a permissioned blockchain approach for enhancing employment integrity in Nigeria. This chapter provides a comprehensive assessment of the literature on blockchain technology and its uses. The section explores the analysis of salary and payroll systems, the development of payment systems, and the fundamental ideas behind them. The chapter also explores the issue of corruption in developing countries. Gaining a comprehensive understanding of these fraudulent strategies equips us to analyze how blockchain technology might effectively address these issues. A comprehensive analysis was provided to gain a thorough understanding of IPPIS and the perspectives of other authors. Moreover, blockchain was examined alongside its fundamental concepts and categories. Finally, vulnerabilities and security in blockchain are explored. The security of blockchain is ensured by its decentralization, immutability, and consensus mechanisms. This chapter serves as a bridge to the subsequent chapters, which will delve into the specific methodologies and experiments conducted in this research to demonstrate the practical applications of blockchain in solving employment fraud issues.

## 2.1 Payment systems

Today's monetary system allows payments to be made with currency and that has eased the process of economic transactions, it has provided convenient platform and

policy through which payment can be made. Currency is money in the form of paper or coins, usually issued by a government and generally accepted at its face value as a method of payment. Payment is considered when an asset or benefit is moved from one party to another in order to discharge a debt. It may also comprise of payer's approval to a third party to make such transfer [65].

On the other hand, Nakajima is of the view that payment refers to the transfer of monetary value between payer and payee [273]. He also opined that a payment system is a systematic procedure for transferring monetary value between parties. Diebolt and Haupert defined payment system as a composite of financial instrument dealings that move value among parties to complete transaction [114]. The reliance of payment systems, laws, practices and institutions that is responsible for such activity is an important factor that makes an economy. According to Boel payment system is the combination of technological devices, laws, and contracts which allow and determine payment settlements [65]. Countries rely hugely on the efficient functioning of such systems.

## 2.2 Evolution of payment systems

The oldest form of money according to Baliga et al. is cattle which existed from the period 9000BC [42]. The system continued until the coming of Agriculture when grain and other vegetables became a standard form of barter in many societies in 6000BC. China was the first country to use cowries as a means of exchange. Cowries are highly polished and brightly coloured shells of a marine gastropod which are found in the Pacific and Indian oceans. For a long time, many societies have used cows as a form of money. Even in the mid 19th century some parts of Africa used cowries as means of exchange. At the end of the stone age in 2000BC, China, using bronze and copper developed cowries of same shape and size. This led to the beginning of metal coins. Thus, the first metal money began in 1000 BC. There were other forms of money developed in 118 BC which was the leather money.

Leather money was also first developed in China and it was the first documented

type of banknote. Banknotes first appeared in China in the 7th Century and were used for over five hundred years before it then went into extinction due to depreciation and inflation. It was not until 1661 before it reappeared in Europe and after three centuries it was considered. Payment systems have developed significantly over the years and it is continuing to advance. In the 19th century, payment system was then evolved from cash-base system in which payments were made in coins to a system where paper check was used [28]. Angel and McCabe argued that the world is progressing because electronic payment is replacing the old method of payment (cash). Meanwhile, Schulte viewed that paper check is lessening quickly [359].

## 2.3 Salary and payroll system

According to Xiaojie, students in the early 13th century in Europe were responsible for their teachers' salaries [431]. The idea of paying salaries from public purse was not popular. Only in the 14th century that the municipal authorities considered yearly salaries but to a few personnel with merit and have contributed immensely. Xiaojie stated that universities in Germany blossomed before the end of 14th century, and this led to instituting salary system [431].

Before the end of the 16th century, many universities adopted the salary system, and from then almost all universities adopted and implemented the salary system. The author stated that the time interval for receiving salaries developed gradually [136]. In the beginning, it was on a yearly basis where contracts were signed under the salary system. It then became a different time interval depending on the arrangement agreed. Salary increment began to surface gradually where a minority of famous professors were considered. Later number of beneficiaries started to expand. After a while, all teachers enjoy increments in salaries though the amount varies. The salary system as viewed by the author was first classified as a custom, it then gained legal and institutional support which developed into a public system. Universities became more dependent on government due to salary system and developed tremendously in terms of infrastructure and staff development due to government making public funds accessible to them [269]

[238].

## 2.4 The evolution of payroll systems

According to Tan, payroll systems have evolved through ages [389]. From the 1980s to 2016 he gave the following as evolution of payroll systems;

In 1890s, Jeweller William Le Grant Bundy invented a time card machine. Workers were equipped with unique keys for access. The idea is to punch theses key in and out during arrival and departure. The timestamps keep track and documents the employees' attendance. From 1920 to 1940, it was a complete manual process where employees submit their time cards to staff who in turn tally hours in ledgers to calculate wages. The system was slow and consequently, payments were delayed.

In the 1950s, Lyon Electronics Office computerized the payroll system. The system invented does not handle payroll system alone but also inventory and labour cost management as well [83]. Lyon became the first company to offer payroll outsourcing services. By the 1980s, payroll and other business services were handled by IBM. With IBM and the involvement of telecommunications services, employees makes submissions without physically coming to office because Fax machines made task easier to transfer scanned documents. In the 90s, when emails and small sized computers began to proliferate, employees found it easy sending data and documents through email. Payroll applications were designed and introduced though data was still captured and entered manually into the system for processing. This led to lots of human error.

In addition, clock systems were used to keep track of time and attendance. Managers monitor and control the coming in and going out of employees because it keeps record and assists during payments [17]. From 2000 to 2016, proximity card readers supported by RFID were used [259]. Employees only wave their cards when having access or leaving workplaces. The devices were embedded with security features in such a way that only authorized personnel could use. Biometric technology played an important role as well. The scanners keep track of time and attendance. The company made the system to manage payroll and HR simultaneously on multiple systems but businesses

are deciding to combine all on a single cloud platform.

## 2.5 Corrupt practices in developing countries

Corruption is the systematic abuse of power for personal gain [230]. It is a major setback that impedes development in Nigeria and other developing countries in Asia [352]. Corruption, theft and other illicit financial flows cost Nigeria and other developing countries more than one trillion GBP annually [137]. The act creates inequality in opportunities by favouring a particular set of people. As resources, capital, projects and other benefits are diverted away from real beneficiaries, development is automatically truncated [271]. Looting monies make infrastructural developments impracticable and subject countries to economic hardship. Substandard infrastructures are constructed due to the corruption engaged in their execution, endangering the lives of the individuals [352].

Transparency International Corruption Perception Index categorized corruption into three, grand, medium corruption and petty corruption. Corruption can be grand when government officials are convoluted in it. In medium, government or private institutions use links for personal incentives, while in petty corruption, individuals are engaged to utilize their power for personal gains [404]. Corrupt practices in developing countries exist in almost every sector of the economy some of which are spelt by the law and possess prescribed punishments. They include public funds embezzlement, bribery, nepotism, electoral corruption, extortion, ghost working etc. Corruption is widely practised in the judiciary, contracts awards, land registry, budgets, education, custom services and many other Ministries and Agencies [290]. Some of these corrupt practices are discussed as follows:

### 2.5.1 Embezzlement of public funds

In every government or organization, embezzlement is the highest type of fraud. It is a common practice where money or other asset is used for personal gain instead of what was appropriated for [265]. According to the Transparency Perception Index (CPI),

Nigeria is the 154 least corrupt out of 180 countries as shown in Figure 2.1 [188]. Money laundering, kickback acceptance and inflating contracts is a common occurrence among top government officers in Nigeria. In May 2022, Accountant General was arrested by the Economic and Financial Crimes Commission (EFCC) in connection with diversion of funds and money laundering activities to the tune of 80 Biliion Naira (43 Million GBP) [213].

The Academic Staff Union of Universities (ASUU) declared that the Accountant General utilized the IPPIS to defraud Nigerian workers and expose them to extreme poverty [104]. In the same vein, a serving senator of the Federal Republic of Nigeria, Senator Rochas Okorocha was arrested in May 2022 on charge with the diversion of public funds and properties to the tune of 2.9 billion Nigerian Naira (2 Million GBP) [184]. Every year Nigeria loses more than 50 billion Naira (28 million GBP) to illegitimate cash flows due to corruption.

The United Nations Economic Commission for Africa reported in 2013 that Africa loses 50 billion dollars to corruption annually (Africa Loses $50 Billion Every Year, 2013). Embezzlement of public funds is the most common form of corruption emanating from various forms of corrupt practices. Hence, it is necessary and important to stop or minimize the act to the barest level for the development of any country.

### 2.5.2 Judicial corruption

Judicial corruption is when court personnel misuses the court and public authority for their benefits. It comes in different forms and methods in developing countries [79]. In Nigeria, judicial corruption is one of the most hidden and most dangerous forms of corruption. It has been said that “why hire a lawyer when you can buy the judge” [347]. In 2021, the Independent Corrupt Practices and Other Related Offenses Commission (ICPC) reported that the judiciary is leading the Nigerian corruption index between 2018 and 2020. The commission claimed that about 9.458 billion Naira (more than 9 million GBP) was paid as bribe by lawyers to the sector [183]. More so, former chief judge of Nigeria, Justice Walter Onnonghen was convicted in 2019 by the Code of Conduct Tribunal (CCT) for false assets declaration and having multiple personal

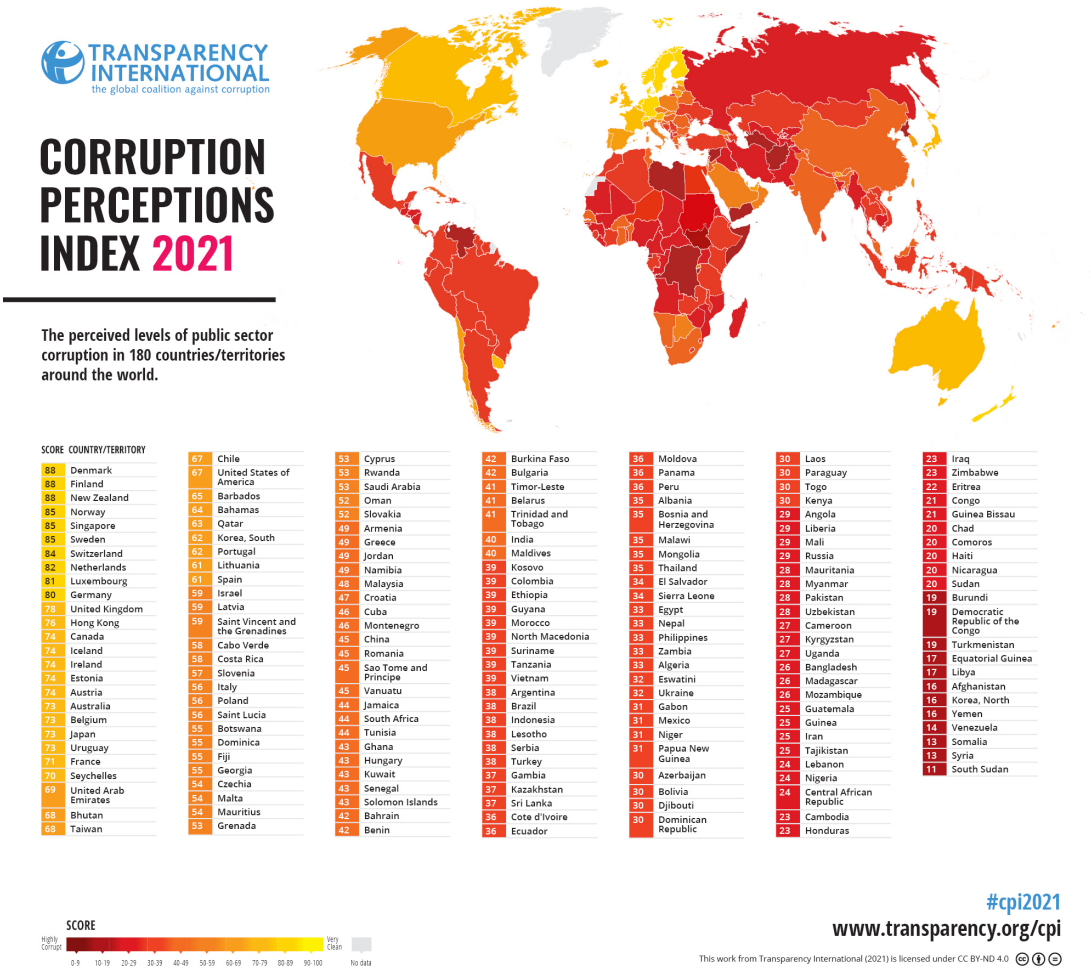


Figure 2.1: Nigeria Corruption Perception Index. Score of 24.
Source: Transparency International, 2021 Report [188]

bank accounts containing billions of Naira (millions of GBP) [422].

### 2.5.3 Electoral corruption

There are two major forms of electoral corruption in Nigeria – vote buying and abuse of power of incumbency [183]. Power of incumbency refers to the advantages that current officeholders (incumbents) have over challengers in an election. These advantages can significantly influence the outcome of elections, especially in political systems like Nigeria's. The business of vote buying right at the polling booth dims the hope of democratic consolidation and it is a current problem of Nigeria's democratization process which is caused by the ruling class [293]. Recently, the UK government raised their concern over vote buying during the Ekiti State governorship election which was held on June 18, 2022. The British High Commissioner remarked that relevant authorities should hold perpetrators accountable, noting that selling and buying votes have no place in a democratic setting [128]. Other forms of electoral corruption include bribing of electoral officers and security personnel to facilitate rigging.

## 2.6 Integrated Payroll and Personnel Information System

Ministries, departments, and agencies (MDAs) are using Integrated Payroll and Personnel Information System (IPPIS), a computerised human resource management information and payroll system, to carry out a variety of human resource-related tasks. IPPIS was implemented as part of public service reform initiatives that sought to improve service delivery and increase accountability by automating human resource tasks and supplying timely, accurate information for decision-making. The Nigerian Government is currently using IPPIS as the platform to pay its employees' salaries and other entitlements [406]. The government was previously using Government Integrated Financial Management Information System (GIFMIS) for the exercise but discovered that the platform was not robust and reliable, the system was opened to ghost workers and used for corruption [406].

However, IPPIS could not solve the issues of the previous system instead the prob-

lem escalated [24]. In the same vein, Ghana, which is also a developing country in Africa is battling with their payroll system. Also, according to Quarm and Rosemond, the current platform cannot identify or detect ghost workers [319]. The Government at the end of the day cannot estimate the huge amount of monies that went down the drain due to the weakness of the payroll system. According to Moshonas, the payroll department in the Democratic Republic of Congo (DRC) only verifies the payroll obligations provided by the Line Ministries, and the payroll technology they use has centralisation problems. Among other things, this resulted in embezzlement, ghost workers, and other omissions [264].

According to Masele and Kagoma, there is a significant breakdown in Tanzania's public universities' payroll system. Workers consistently experience salary delays, and there have been several reports of inadequate financial accountability. Approximately 19,700 ghost workers were found in the payroll system, and there were multiple instances of overstated wage bills and ghost workers. This shows unequivocally that the Human Capital Management Information System (HCMIS) does not guarantee data accountability and integrity.

The impact of IPPIS on the sustainability of higher education in Nigeria following the COVID-19 pandemic was investigated by Emanghe and Amoramo. According to the report, accurate budget estimations and the eradication of payroll fraud have a substantial impact on university education in Nigeria following the COVID-19 epidemic. To ensure sustainability, the authors suggest automating the process of estimating university budgets [130]. In a 2020 study, Paul and Grace examined the relationship between electronic governance and corruption in Nigeria, drawing on insights from IPPIS implementation [309]. The authors explored how IPPIS minimises corruption in the Nigerian public service. They noted that there are mixed feelings about its effectiveness. However, the report recommends that the application be expanded to include all MDAs. They urge that users be regularly trained and encouraged to be upright while carrying out their responsibilities.

In a separate study, Uzoh discovered that the adoption of IPPIS infringed university autonomy [406]. He believes that the federal government should exempt colleges

from the IPPIS platform since it has not addressed their unique needs [406]. In the meantime, Abdulsalam Nasiru et al. studied the influence of IPPIS on transparency in government payroll administration in the Nigerian Civil Service [4]. It was a descriptive cross-sectional survey research design, with questionnaires distributed. It was revealed that IPPIS has a substantial association with transparency and accountability. The authors urge that the government expand IPPIS's internal control mechanism in order to combat fraud on a continuous and effective basis, as well as conduct routine audits and inspections of the application [4]. The paper also suggests that strict compliance with laid down rules governing IPPIS and compliance with the provision of the Financial Regulations and the Civil Service rules.

### 2.6.1 Overview of the standard operating procedures of IPPIS

An examination of the IPPIS Standard Operating Procedure (SOP) document was done in order to obtain a thorough grasp of the current procedures and to evaluate the possibility of incorporating blockchain technology for transparent employment process and to stop ghost worker fraud. The `Payroll & Payment Standard Operating Procedure` SOP document offers a thorough explanation of the payroll and payment procedures that are overseen by the IPPIS department [391].

The document explains the operational framework that controls payroll administration for all Ministries, Departments, and Agencies (MDAs) that have adopted the IPPIS platform. It covers timelines, roles, and responsibilities for all the steps in the payroll processing process, from the initial data collection to the last employee payment [391]. This extensive procedure consists of several levels of verification and tests to ensure accuracy and to stop fraud.

#### Key elements of the IPPIS SOP relevant to fraud prevention

The SOP emphasizes various crucial components important for combating fraud, including ghost worker fraud, which is described as the placement of non-existent employees on the payroll for fraudulent purposes. The methods outlined in the document are intended to provide strict control over payroll data and transactions [391]. Some

significant elements are:

**Controlled payroll periods:** The SOP provides that payroll periods begin on the 25th of the current month and finish on the 24th of the following month. This regulated period reduces the opportunity for unauthorized changes to payroll data.

**Role segregation:** The document emphasizes the need of duty segregation in the payroll process, with various staff (Initiator, Reviewer, and Finaliser) assigned specific responsibilities to prevent unauthorized access and fraud. This separation of roles ensures that no single person has complete control over the payroll process, decreasing the possibility of fraud.

**Pre-payroll and post-payroll meetings:** The SOP mandates pre-payroll and post-payroll meetings involving key stakeholders, such as Payroll Solution Providers and the Payroll Committee, to review and approve all payroll data and adjustments. These meetings serve as checkpoints to verify the accuracy of payroll data and to detect any irregularities that might indicate fraudulent activity.

**Audit and quality assurance:** The SOP requires pre and post payroll meetings with key stakeholders, including Payroll Solution Providers and the Payroll Committee, to evaluate and approve all payroll data and adjustments. These meetings serve as checkpoints for ensuring the accuracy of payroll data and detecting any inconsistencies that could suggest fraudulent conduct.

**Digital record-keeping and reporting:** The SOP requires all payroll transactions and processes to be digitally documented, with reports provided for various stakeholders. This digital record-keeping increases transparency and creates an audit trail that could be utilized to detect fraud.

### Summary of Weaknesses of IPPIS

The IPPIS was introduced to address ghost worker fraud and improve payroll efficiency. Despite improvements, significant weaknesses persist. Some are as follows:

1. Centralization: IPPIS is managed by a small group of central administrators. This creates a single point of failure, where insiders may insert ghost workers or alter records undetected.

2. Manual processes: Data entry and verification remain partially manual, relying on HR officers and payroll officers. This introduces human error and opportunities for collusion.

3. Limited verification: The system operates largely within its department, without external validation against errors or frauds.

4. Opaque validation and delayed audits: The validation process includes pre- and post-payroll meetings but lacks independent external oversight. Fraud may remain undiscovered until periodic audits.

5. Inconsistent enforcement of SOPs: Even though SOPs exist, enforcement varies across MDAs, leaving gaps in fraud prevention.

## 2.7 Some technologies capable of curbing ghost worker fraud

Several technologies have been developed to enhance payroll integrity and reduce fraudulent practices such as ghost worker schemes. These solutions aim to improve verification, transparency, and accountability within employment systems. This section provides background on some of these relevant technologies, which include Public Key Infrastructure (PKI), centralized relational databases with advanced auditing, biometric authentication systems, robotic process automation (RPA), secure multi-party computation (SMPC), and digital identity management platforms. The subsequent section then presents the selected technology for this project.

### 2.7.1 Public Key Infrastructure (PKI)

PKI uses asymmetric cryptography to issue and manage digital certificates, ensuring that only authorised users can submit or approve payroll data [9]. Digital signatures under PKI can help track who added or modified records. However, PKI typically depends on centralised certificate authorities [72]. If compromised, they become a single point of failure, undermining trust and can also lead to security vulnerabilities and scalability issues [72].

### 2.7.2 Centralised relational databases with advanced auditing

Modern databases (e.g., Oracle Audit Vault, PostgreSQL with pgAudit) can enforce strict access controls and generate tamper-evident logs [306]. They can also support role-based access to limit who can add employees to payroll. However, they remain inherently centralised, and administrators with high-level privileges may still manipulate data undetected [338].

### 2.7.3 Biometric authentication systems

Integrating biometrics—such as fingerprint, iris, or facial recognition could verify the physical presence and uniqueness of employees, reducing duplicate or ghost entries [191]. Yet biometrics address identity verification, not data governance; administrators may still bypass controls or collude to insert false records [314].

### 2.7.4 Robotic Process Automation (RPA)

RPA uses software robots to automatically cross-check employee records. In human resource management, RPA can improve service quality, reduce costs, and increase operational efficiency by automating processes like gathering, storing, and accessing employee information [256]. This reduces human error and speeds up validation [11]. However, RPA tools rely on the correctness of input data and the integrity of the databases they query. They do not address deeper issues of internal fraud or manipulation [175].

### 2.7.5 Secure Multi-Party Computation (SMPC)

Secure Multi-Party Computation (SMPC) is a cryptographic technique that enables multiple parties to jointly compute functions on private data without revealing individual inputs [442]. It has applications in various fields, including healthcare, finance, and social sciences, where collaborative data analysis is crucial [19]. This approach maintains confidentiality while ensuring collaborative validation. However, SMPC protocols are computationally expensive and complex to implement at scale, particularly in resource-constrained public sector environments [78] [5].

## 2.8 Blockchain technology

Blockchain technology is a disruptive technology that transforms the information system [49]. It is the foundation upon which Bitcoin, Ethereum, and other digital currencies operate. Blockchain is a distributed and decentralised system that stores and updates records, events, and transactions [369]. The technology could reduce central controls that grant power to a select few, which could help manage a number of security issues [442]. Cryptographic hash functions and digital signatures ensure data security and integrity, making it potentially more safe than traditional centralised systems [284]. Hashes serve as unique identifiers for data blocks and ensure data integrity and security. They are one-way functions that compress an arbitrary amount of data into a short-fixed length deterministically random string [61]. Each block's hash is calculated using the preceding block's hash as well as the contents within the block. This means that hash values are unique and potentially prevent scams, because altering a block in a chain must change the respective hash value [284].

Blockchain ensures immutability, auditability, and traceability which was one of the reasons industries were embracing the technology over the past years [64]. Numerous industries in manufacturing, oil, construction, mining, etc are already cultivating the benefits of blockchain [227]. The realization of blockchain was initially attained around Bitcoin, which is the most successful cryptocurrency put forward by Satoshi Nakamoto in 2008 [275]. The platform has made a long stride in financial institutions. Banking,

Fintech, Insurance, Consumer Finance, Housing Finance, etc., have invested and are benefiting hugely from the blockchain [302]. The global cryptocurrency market cap was 2.41 trillion dollars as of June 2024 [139].

Despite the positive trends of blockchain, the technology has its uncertainties. Yeoh reported that millions of dollars were laundered by Liberty Reserved which Financial Task Force exposed in 2015 [437]. This was as a result of blockchain bitcoin not being included among policymakers and regulators. Blockchain is also open to numeraous cyber-attacks [22] [6], some threats and vulnerabilities were discussed in section 2.9 of this study. Equally, Abu-Elezz et al. believe that attackers can take charge of the blockchain network [7]. They could prevent or even reverse transactions. The authors asserted that the technology lack regulations by legal authorities. Scarcity of technical skills also truncates the operations and acceptance of the technology. Kassab et al. also argued that blockchain consumes a lot of energy and has a slow processing speed [200].

### 2.8.1 Why blockchain is selected

Blockchains are promising digital technology that brings together networking, data management, cryptography, and incentive mechanisms to strengthen the checking, execution, and recording of transactions among users [434]. It refers to a decentralized, open and transparent system where information cannot be altered, and data can be shared by all members [418]. The technology improves transparency, accountability and limits fraud in record keeping at the same time having the ability to create immutable ledgers [413]. The United Kingdom Government Office of Science stated that blockchain ensures data records, lessens operational costs, and delivers transparency in transactions [132]. Some crucial features of blockchain include:

#### Transparency and traceability

Records are stored on every peer on a blockchain network and time-stamped to keep time and dates of transactions. The peers on a permission blockchain networks are linked together so transactions and other activities are quite traceable. From the beginning to the end of processes, peers in the network are involved and as such records can

be traceable and cannot be modified [390]. Transparency, traceability and trust make blockchain a perfect tool for auditing and government digital reforms [164]. Therefore, this feature will assist in preventing employment fraud and ensure compliance and due process law is followed.

#### Distributed and decentralized nature

Blockchain, as a decentralized system eliminates intermediaries and central control (depending on the type of blockchain) making it flexible structure. Even though other blockchain architectures like Permissioned Blockchain may be partially or fully centralized, nevertheless, it benefits from other features of blockchain [284]. Storing and accessing data and information by different users across networks make the system distributed. Thus, a distributed and decentralized system will grant authority to other stakeholders engaged on employment process and that will reduce or eliminate ghost workers since employment will not be made by a selected few. In addition, if a node loses data, other nodes on the network still possess copies of the data and updates the affected node. This function prevents data loss or tampering of records.

#### Efficiency

Blockchain makes processes easier and faster because it allows systems to work autonomously. This feature will easily detect errors during employment process making it transparent and seamless. This is one of the numerous reasons some countries, organizations, and companies are now employing blockchain [215].

#### Verifiability

Transactions on Permissioned blockchain are verifiable, giving room for smooth auditing of records. Equally, transactions on permissionless blockchains are also fully verifiable in terms of correctness and integrity. While permissionless blockchains are often associated with pseudonymity, they are not inherently devoid of accountability mechanisms. Certain permissionless systems incorporate privacy-preserving features alongside traceability options under defined conditions [400]. However, in permissioned

blockchain environments, accountability is typically easier to enforce due to identifiable validators, governance controls, and institutional oversight structures [171].

#### Data Integrity

Data integrity refers to the assurance that data and information remain at its original state and represent what it is being intended [68]. In blockchain network, the hash of each block is generated from the hash of the previous block and the data within the block. Therefore, modifying data on blockchain is not possible without modifying other blocks linked to it.

#### Auditability

Auditability is the ability of an auditor to study and examine a system and get accurate results seamlessly. In payroll management, absolute auditing identifies compliance issues, spots human errors, detects vulnerabilities for fraud etc. Blockchain allows peers to make decision based on all transactions that have happened in the past, not just based on random samples. Blockchain enables auditors to get some level of assurance on what occurs simultaneously with, or shortly after, information discovery [97].

#### Conclusion

While these technologies strengthen specific aspects of payroll amd employment integrity such as identity verification, anomaly detection, or process automation, they generally remain centralised or reactive. Blockchain, by contrast, combines decentralisation, immutable logging, and distributed consensus, making fraudulent payroll entries both harder to insert and easier to detect [51] [444] [92]. As a result, blockchain provides a more comprehensive solution to systemic ghost worker fraud.

### 2.8.2 Cryptography in blockchain

Cryptography is generally termed the study and practice of techniques to secure communications. Its core principle includes Confidentiality, Integrity, Authentication, and

Non-repudiation [101]. The blockchain relies on cryptography to achieve data security and integrity. The SHA-256 is the cryptographic hash function that sometimes the blockchain uses for its consensus algorithm [353]. Bitcoin uses the SHA- 256 and RACE Integrity Primitives Evaluation Message Digest (RIPEMD160) hash function to produce addresses (Sanka et al., 2021). The blockchain also utilizes the Elliptic curve digital signature algorithm (ECDSA) to create, sign and verify transactions, while the Merkle tree is applied to build the hash of all transactions within a block [204].

Some of the most important types of cryptography used for blockchain security are hash functions, public key cryptography, and elliptic curve cryptography (ECC). In cryptography, hash functions are typically used as a one-way function where it's easy to go forward (input to output) but computationally infeasible to go backward (output to input). While Non-Locality ensures similar inputs to a hash function create dissimilar outputs. Another type of cryptography is the Public Key Cryptography, a type of encryption algorithm that uses a different public and private keys. A user generates a pair of these keys which are mathematically related, keeps the private one secret, and publicizes the public one. Public-key cryptography algorithms are designed to make it computationally infeasible to derive a private key from the corresponding public key. Elliptic Curve Cryptography is also a type of cryptography that uses a hard problem that is mathematically equivalent to the discrete logarithm problem for security. Its main advantage is that it has a similar level of security to traditional public key cryptography algorithms while using smaller keys.

### 2.8.3 Blockchain architecture

Blockchain provides a trustless computing infrastructure to solve fundamental trust issues and allows economic transactions to take place smoothly and efficiently [433]. Trustless computing is an emerging paradigm that leverages blockchain technology to create secure, decentralized systems without relying on intermediaries [429]. The approach could address challenges in transparency, security, and privacy preservation [244]. The structure represents a collection of blocks with transactions in a specific order. Each peer in a network creates, authorizes and maintains new entries.

The blockchain architecture is composed of six layers [432]. They include the application layer, contract layer, incentive layer, consensus layer, network layer, and data layer. Figure 2.2 summarizes the descriptions and functions of these layers.

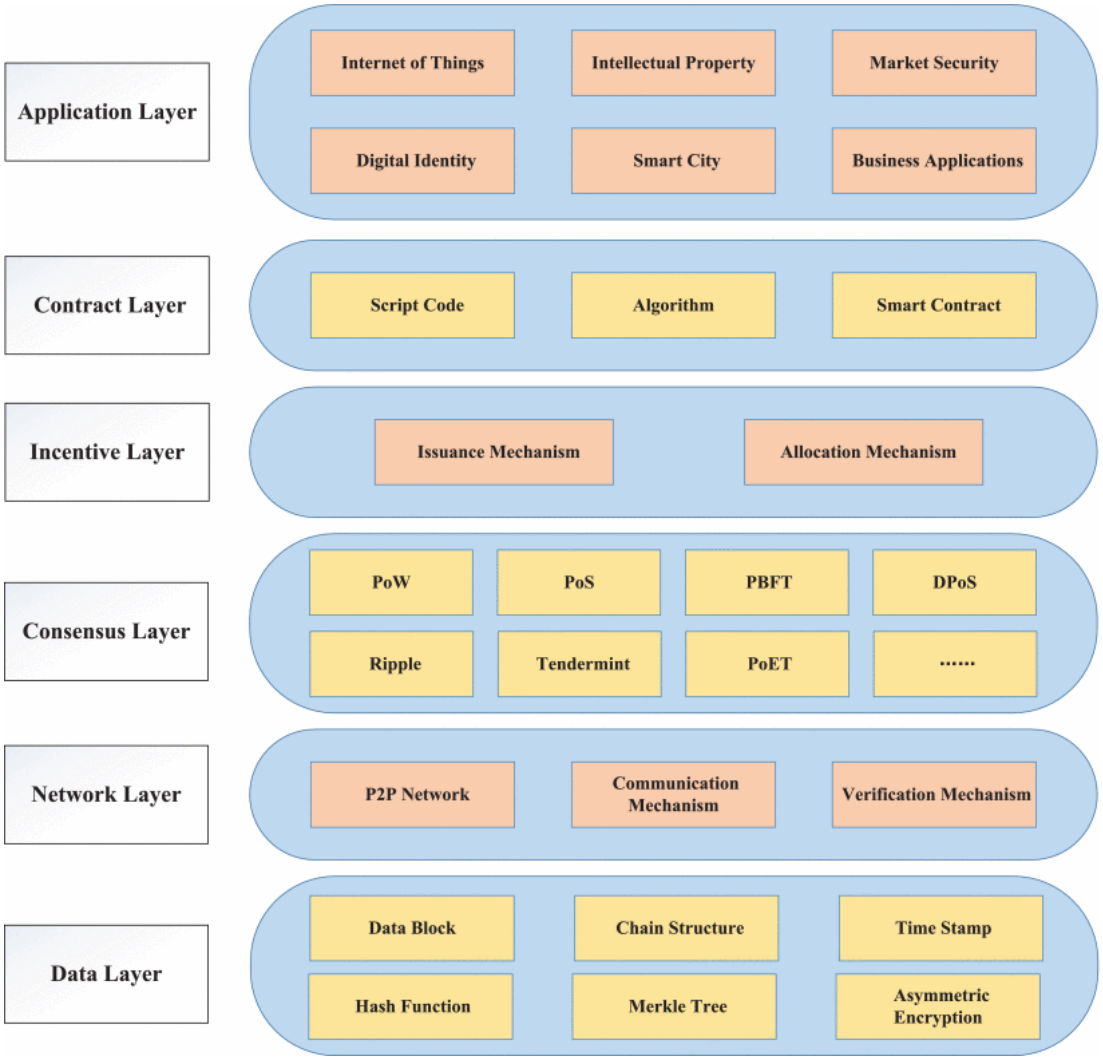


Figure 2.2: Blockchain Six-Layered Architecture
Source: A Survey of Blockchain Technology Applied to Smart Cities [432]

1. Application Layer

   Application is the highest layer in the blockchain architecture and is composed of applications such as market security, health records, land records, IoTs etc [61]. The layer accommodates programs that end users use to communicate across the

blockchain network.

2. Contract Layer

   The Contract layer is where programming activities take place. Different scripts and smart contracts are applied to allow more complex programmable operations. Smart contracts control users' digital assets, express business logic and formulate participants' rights and obligations [210]. Smart contracts allow distrusted parties to transact without trusted third parties.

3. Incentive Layer

   Incentive Layer is designed to motivate miners for contributing their efforts for verifying data and transaction. Miners are participants who validate and add new transactions to the blockchain in proof-of-work systems like Bitcoin and other similar settings. They do this by solving complex mathematical puzzles, which requires significant computational power. The first miner to solve the puzzle gets the right to add a new block to the chain and is rewarded. Digital currencies are rewarded to the corresponding miner once a new block is generated [432], however, miners must still be rewarded even if the blockchain is not based on cryptocurrency and this presents a challenge [179].

4. Consensus Layer

   Consensus Layer is the fourth in the blockchain architectural stack. It is the main layer in which consensus protocol is configured to agree on how a new block is added on blockchain network. The algorithm is responsible for solving issues of trust [300]. Enforcement of network rules that describe the nodes within the network is determined here. Peers are responsible for updating and maintaining the ledger in compliance with a particular consensus algorithm. The algorithm sets out rules on how and who creates new blocks. There are several consensus algorithms implemented on blockchain networks such as Proof of Work (PoW), used by Bitcoin, requires miners to solve complex mathematical puzzles, consuming significant energy but offering strong security [443]. Proof of Stake (PoS),

adopted by Ethereum 2.0, selects validators based on the amount of cryptocurrency they stake, reducing energy use and increasing scalability [38]. Delegated Proof of Stake (DPoS) improves PoS by allowing users to vote for delegates who validate transactions, enhancing efficiency but introducing some centralization. Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm designed for systems with known participants, achieving fast finality and resilience against malicious actors, but it doesn't scale well [334]. Lastly, Proof of Elapsed Time (PoET), developed by Intel, uses trusted hardware to randomly select block producers based on wait times, aiming to mimic PoW's fairness with lower energy consumption [69]. They are responsible for making sure nodes come to same terms on transactions and the present state of the ledger [197]. The consensus layer ensures that peers in a network reach consensus in the network domain and nodes status remains the same [433].

5. Network Layer

   The Network Layer is comprised of the distributed networking mechanism, communication mechanism and data verification mechanism. The layer is responsible for the distribution and verification of blockchain transactions [432]. A peer-to-peer network is used to broadcast transactions among peers.

6. Data Layer

   In blockchain architecture, the Data Layer serves as the system's foundation, organising and storing the blockchain's basic components. This layer contains the actual data that makes up each block, as well as key cryptographic components such as digital signatures, hash pointers, and the Merkle tree structure [1]. These features protect the data's integrity and security by establishing verifiable links across blocks, making it hard to tamper with previous data without detection. This layer also includes algorithms utilized in the process, such as hashing functions, which provide secure data handling over the blockchain network. The Data tier, being the blockchain stack's lowest tier, serves as the foundation for higher layers such as the consensus and application layers to work. This layer

ensures the immutability of the blockchain by securely linking blocks, resulting in a tamper-resistant chain [301]. Each block in this layer carries the previous block's cryptographic hash, resulting in a sequential and immutable chain. As a result, the Data Layer is critical to ensuring the overall transparency, security, and integrity of the blockchain system.

### 2.8.4 Blockchain structure

A blockchain is a monotonically growing list of records called blocks, connected and secured using cryptography. Each block contains transaction data, timestamp, and cryptographic hash function of the previous block [197]. Hashes are used as unique identifiers for data blocks and to establish data integrity and security [61]. The hash of each block is generated from the hash of the previous block and the data within the block. This implies that hash values are unique and that can prevent scams since alteration of a block in a chain must alter the respective hash value [284]. The first block in the chain is referred to as the genesis block. The blockchain structure comprises a block header and block body (transaction data). The header encapsulates the timestamp, Merkle root, and other components including the previous block hash [445].

A block consists of the block header and the block body as shown in Figure 2.3, the block header includes: (i) Block version: specifies and directs which set of block validation rules should be followed. (ii) Merkle root: encodes blockchain data efficiently and securely. It is the hash value of all the transactions in the block. It facilitates quick verification of data and enables the transfer of data from one node to another [361]. (iii) Timestamp: shows the date and time a new block is created and each transaction that occurs. Timestamps minimize double-spending and alternations. They also preserve the integrity of blockchain. (iv) nBits: target threshold of a valid block hash. The target is inversely proportional to the difficulty and is encoded as a compact representation of a 256-bit number [268]. (v) Nonce: an 4-byte field of random numbers used only once by miners to calculate for a new block on the blockchain. It increases for every hash calculation.

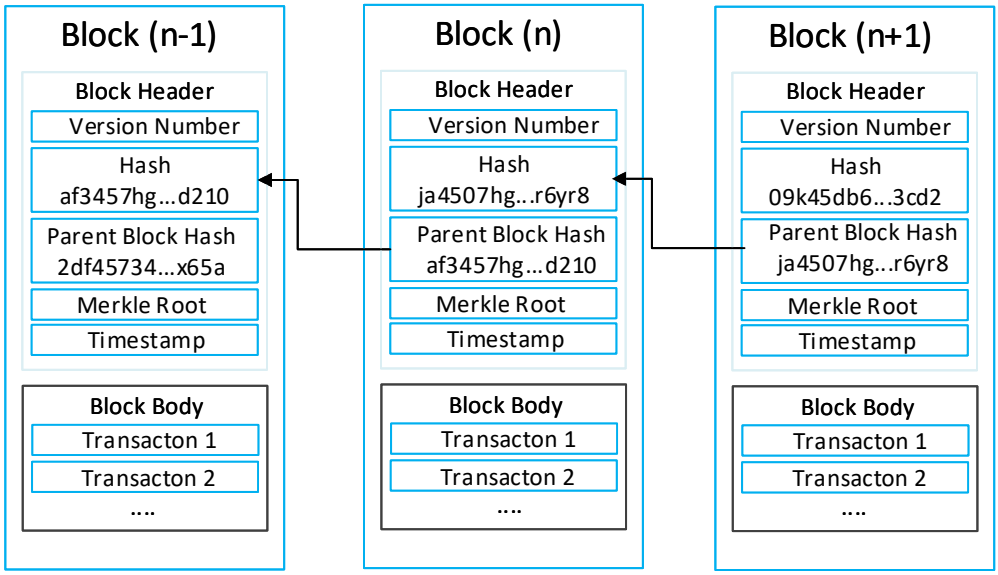


Figure 2.3: Blockchain Structure

### 2.8.5 Classification of blockchain

According to Buterin, blockchains are classified into two types; permissioned and permissionless. The private and consortium blockchains are regarded as permissioned while the public blockchain is viewed as permissionless [80]. The two types are discussed below:

#### Public (permissionless) blockchain

In this type of network, any peer could join and leave the system anytime without restrictions, and they could also add and verify transactions. The network is open and decentralized as depicted in Figure 2.4. There is no central authority that controls or manages membership [430]. Bitcoin, Ethereum and other cryptocurrencies are typical examples of public blockchains. New blocks are usually obtained through mining which peers must compete for. Public blockchain is not immune to cyber threats, the commonest among them is the 51 percent attack and the double spending attack [228], further discussion on threats and vulnerabilities are found in section 2.9.

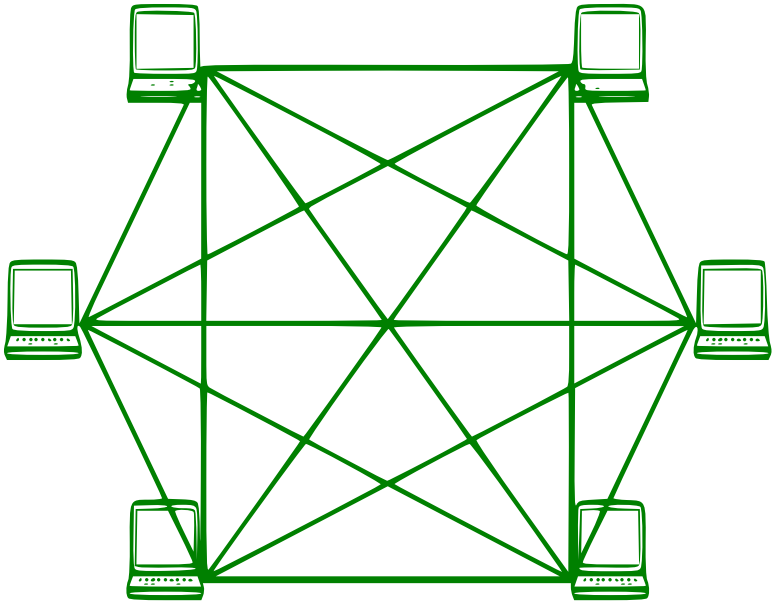

Figure 2.4: Public (Permissionless) Blockchain
Source: An overview of blockchain and consensus protocols [348]

### Private (permissioned) blockchain

The private blockchain is also open and decentralized as the public blockchain, but here, any participant must be authenticated and authorized. The system only allows limited selected peers, see Figure 2.5. The central entity decides who to join and what role to play [154]. The network is mostly used within single companies or organizations with lesser complications or threats than the permissionless ones [228]. Hence, privacy in private blockchains is mainly achieved through access control where only authorized participants can join the network, view data, and validate transactions. Privacy is also achieved through selective disclosure where sensitive personal data can be encrypted or stored off-chain, with only verification proofs recorded on-chain. In addition, data partitioning also gives data privacy because data can be segmented in such a way that only relevant parties have access to certain details.

### Consortium (permissioned) blockchain

Consortium blockchain limits the scope of decentralization and openness in a network [393]. The architecture, to some extent, is a hybrid of the private and public blockchain

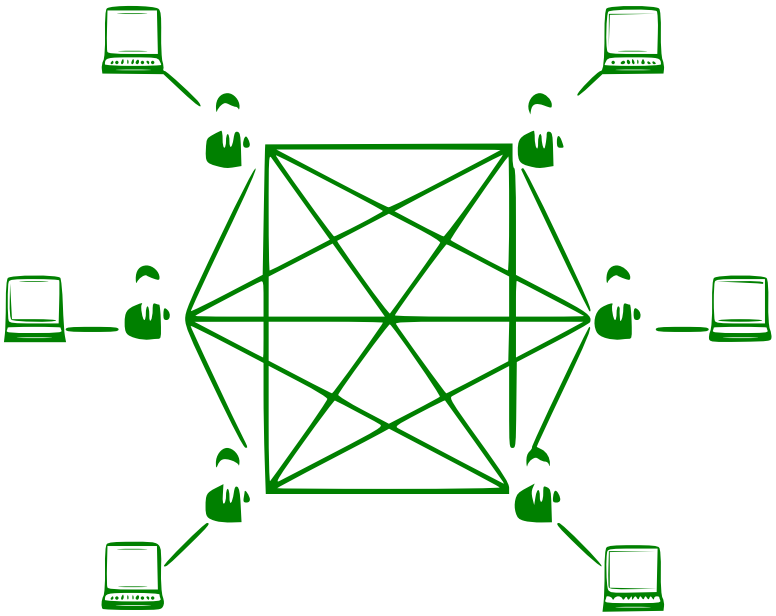

Figure 2.5: Public (Permissioned) Blockchain
Source: An overview of blockchain and consensus protocols [348]

[435] because some peers are selected to participate in consensus and validate new blocks while others are only privileged to read permission [352]. Groups of organizations, government agencies, and companies as consortium use consortium blockchain. Hyperledger, Quorum, Ripple, R3, Multichain, Corda etc are all examples of consortium blockchain [352].

### 2.8.6 Private blockchain networks

Private blockchain networks permit government and organizations manage their data and operations effectively and securely. Private blockchains require explicit permission to participate as a node. Numerous researchers and developers have used the private Ethereum blockchain. Hossain et al. proposed a blockchain-based automated tax return verification system for Bangladesh government using the Private Ethereum blockchain [176]. The idea is to curb corruption in many sectors of the government. In the proposed architecture, taxpayers' information is not only secured but filed tax returns are verified instantaneously. Hossain et al. utilized Ganache as the localhost blockchain server, Metamask for bridging web browsers, and Remix solidity to write Solidity smart

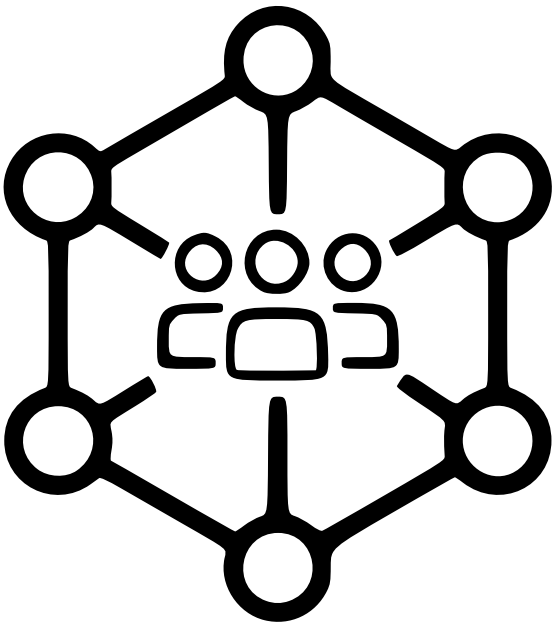

Figure 2.6: Consortium (Permissioned) Blockchain
Source: Types of Blockchain: Public, Private, or Something in Between [419]

contracts [176].

Nicoletti et al. developed Cloud Federation-as-a-Service solution empowered by blockchain technology for the Italian Ministry of Economy and Finance [282]. The aim is to obtain a cross-cloud application for calculating the police force paylip. The application has been implemented and adopted as part of the Italian Public payroll system. In the same vein, Giri et al. discusses how blockchain technology could be used to solve the problems of the payroll system in underdeveloped countries [149]. The result revealed the challenges including ghost work fraud, decentralization, cybercrimes and other human manipulations. They conducted a thorough review of the current literature and demonstrated the importance of the application of blockchain technology to payroll systems.

Our research uses private Ethereum Besu blockchain frameworks to let government agencies interact and transact securely while protecting data. By creating a private blockchain network for the validation and approval of new employees, we can preserve sensitive data while ensuring transparency and accountability.

### Consensus algorithm

Consensus may eliminate problems with trust and improves the efficiency and transparency of processes. Blockchain technology was not the first to use consensus algorithms; Eisenberg and Gale discovered them in 1959 long before the existence of the blockchain [127]. The two categories of the algorithm were the non-byzantine fault-tolerant Algorithm and the Byzantine fault-tolerant Algorithm. Viewstamped Replication (VR) and Paxos are a few examples of non-Byzantine fault tolerant algorithms [44], while Byzantine Fault Tolerant algorithms include Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA) and others [44].

**Byzantine generals problem:** Lamport et al. initially examined the Byzantine General Problem and the challenges that develop as a result of the propagation of false information that is not consistent in different areas of a system [217]. The topic was centered on distributed systems that could be damaged to the point of failure due to network communication failure. The article depicts the consensus dilemma as army generals preparing to attack a fortified city, but among their ranks are traitors. Only if the loyal generals and their troops decide to attack the enemy city at the same time can the Byzantine army win. As a distributed system, blockchain technology is afflicted by the Byzantine Generals Problem; several algorithms and consensus techniques have been created to address this issue.

According to the Byzantine General Problem, an army represents a blockchain network, and a general can be a node in that network, relaying messages to other generals/nodes via a messenger. To avoid misinformation, all active generals should exchange the commands they receive, and the generals would make the final decision based on deterministic probability. This technique, however, is flawed if the generals receive different directives or if more generals decide to lie about what they received, and as the army grows in size, the vulnerability surface grows [442]. Due to the chances of system failure when the system expands and goes into production, this difficulty leads to hard decisions when selecting Blockchain technology and consensus algorithms to use.

## 2.9 Blockchain security, vulnerabilities and attacks

The objective of this section is to present and describe basic blockchain security, consensus security, smart contract security, and the different types of blockchain vulnerabilities and attacks. Blockchain, by design, has its security elements such as its distributed nature of data storage based on consensus and cryptography [340]. Blockchain security is obtained through the implementation of a cybersecurity framework, testing methodologies, and the adherence to coding practices [386]. There are different levels of vulnerabilities and attacks on blockchain networks and this depends type, design and location. Howard and Kris categorized the levels into three; network-level vulnerabilities, system-level vulnerabilities and Smart Contracts Vulnerabilities [177]. These vulnerabilities and attacks by Howard and Kris are discussed in the following sections;

### 2.9.1 Network-level vulnerabilities

In the blockchain's network physical level, there are points that could be vulnerable and attacked. Below are some of vulnerabilities that could be exploited;

#### 51 percent attacks

A 51 percent attack is one of the simplest possible attacks against the blockchain, since it takes advantage of the legitimate function of the consensus algorithm [357]. In a Proof-of-Work blockchain, the state of the blockchain is determined by majority vote since, in the event of a divergent blockchain, the branch having the greater amount of work behind it wins. If an attacker controls 51 percent of a PoW blockchain's computational resources, they control the blockchain [357]. Performing a 51 percent attack requires an attacker to purchase, rent, or steal enough computational resources to have more than the rest of a blockchain network put together [357]. Once they control the blockchain, they can perform double-spend attacks [177].

Checkpointing is designed to protect against 51 percent attacks, and it is done by storing a block in the history of the blockchain at intervals and refusing to accept divergent blocks without these blocks, they prevent an attacker from rewriting too much

of the ledger's history [177]. However, divergent blockchains can exist legitimately, so there is a fine line between protecting against attack and legitimate operation of the blockchain. Checkpointing also runs the risk of splitting the network. That is, if there is no unanimous agreement among all nodes on the checkpoints, it might result in a division within the network, where various parts of the blockchain adopt different historical records. A fork, also referred to as a split, has the potential to divide the network into several blockchains that are not compatible with each other. This can weaken the overall integrity and cohesion of the blockchain system [177].

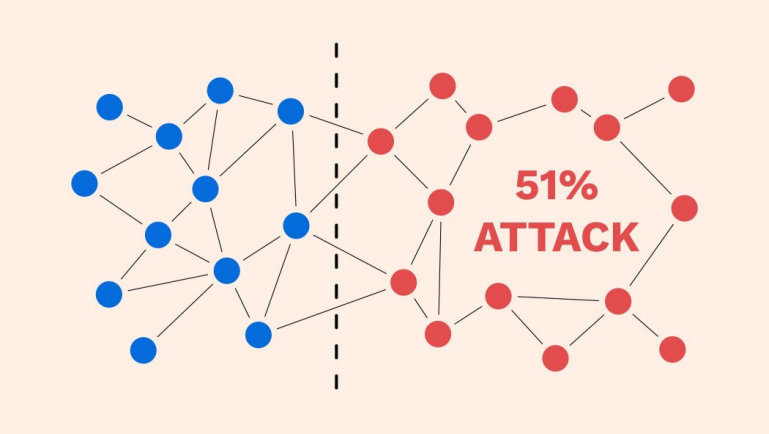


Figure 2.7: 51 Percent Attack
Source: Bitpanda, 2022 [62]

### Denial of service attacks

In a Denial of Service attack, an attacker attempts to degrade a service's operations or make it completely nonfunctional [177]. In traditional, centralized networks, Denial of Service Attack targets the network's bottlenecks or single points of failure. Blockchains are designed to be decentralized and have no single points of failure, but denial-of-service attacks can still be effective against them. A typical example of DoS attack is shown in Figure 2.8. The details of a Denial of Service attack depend on the blockchain technology and where bottlenecks and single points of failure arise in its operations [177]. Examples of Denial of Service attack types include Transaction Flooding, Artificial Difficulty Increase, Block Forger DoS, and Permissioned Blockchain

MSP DoS. The various types of Denial of Service attacks can be mitigated in different ways based on how they are implemented. For transaction flooding, one should intentionally create blocks to clear flooded transactions from the queue while artificial difficulty increases, setting difficulty increase interval to minimize attack impact. PoS and MSP DoS, implementing traditional DoS protection for nodes [177].

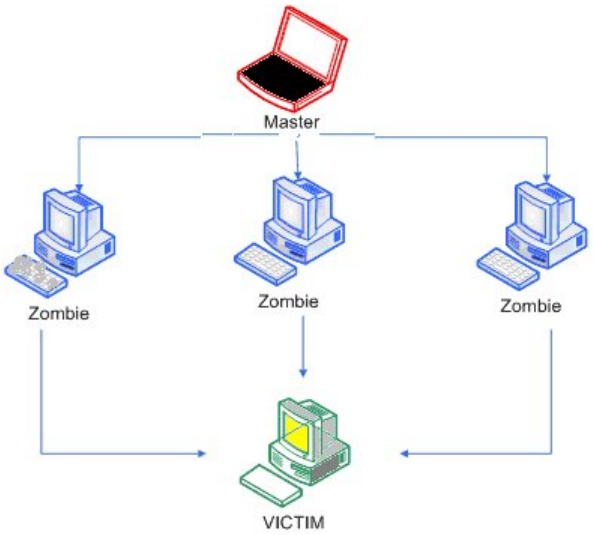


Figure 2.8: Denial of Service Attacks
Source: Impact of Attack Vectors in Cloud Networks [354]

### Eclipse attacks

Blockchains run on a peer-to-peer network where each node connects to several other nodes. The network is deliberately not fully connected since this would dramatically increase overhead [177]. In an Eclipse attack, an attacker controls all the connections of a node to the network, allowing the attacker to completely control the node view of the distributed ledger and network operations, as shown in Figure 2.9. A successful eclipse attack allows the attacker to perform a double-spending attack against the isolated node, helps the attacker perform a denial of service attack, or allows the attacker to use the node's computational resources for the attacker's benefit in the blockchain consensus algorithm [177].

A successful eclipse attack requires the attacker to have location, power, scale, or malware at their disposal [177]. Location is helpful in this type of attack because an attacker may be able to intercept the user's messages before they reach the rest of the blockchain network by Wi-Fi, physical access to network cables, etc. If an attacker has the power of an ISP or similar, they have complete control over user communications. An attacker with significant resources could implement a large-scale attack in which he or she creates many accounts on the blockchain in the hope that all the user's randomly selected connections will be to attacker-controlled nodes [177]. Finally, the attacker could infect the user's computer with malware and use this to control their communications.

The probability that an eclipse attack will be effective can be reduced in a variety of different ways [177]. Firstly, through increased connections, this reduces the probability that an attacker can control all nodes to which the user connects. Secondly, through whitelisting, this is to have a list of known, trusted nodes and always link to at least one. Random reconnections also improve the probability that, if eclipsed, the attack will be short and detectable [177]. Finally, permissioned or private blockchain design decreases the likelihood of malicious nodes on the network and makes scale-based attacks more difficult since membership is invite-only.

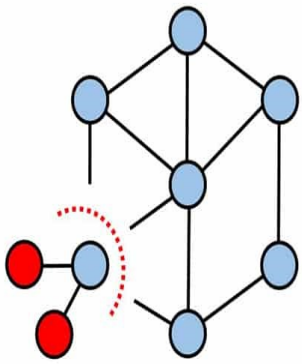

Figure 2.9: Eclipse Attacks
Source: What is an Eclipse Attack? [178]

### Replay attacks

Transactions on the blockchain include the sender's digital signature. This is to ensure that the transaction was generated by the sender and has not been modified in transit [177]. An attacker cannot forge a digital signature, making it impossible to generate fake transactions. In a replay attack, an attacker takes an existing transaction and re-submits it to the blockchain as a new transaction, as shown in Figure 2.10. Since the original transaction was legitimate, the digital signature will be valid and acceptable to the blockchain. This type of attack could benefit the attacker if the initial transaction benefited the attacker. The attacker gets paid twice by replaying a transaction [177]. To protect against this attack, a blockchain can include nonces (number used once) in each transaction. If a replayed transaction should have a new nonce and does not, it will be rejected. If an attacker tried to change the nonce value and replay it, the digital signature would be invalid and rejected by the network [177].

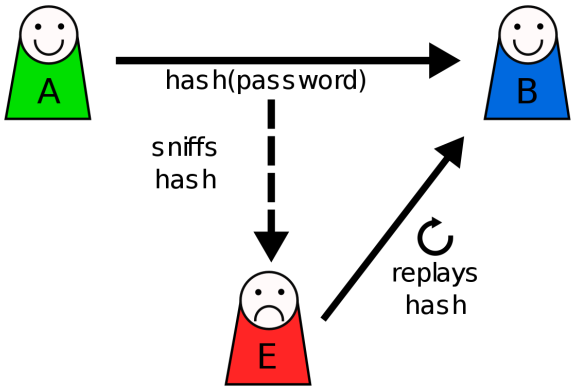


Figure 2.10: Replay Attack
Source: Replay Attacks On Hash [421]

### Routing attacks

Unlike most blockchain attacks, routing attacks target the underlying communications network used by the blockchain for peer-to-peer communications. If an attacker can control all communications between two sets of nodes, they can partition the network

[177]. This is useful in performing 51 percent attacks, Denial of Service attacks, and double-spend attacks. Routing attacks are only successful if an attacker can control all connections between the two parts of the partitioned network. Several methods can decrease the probability of a successful attack; multi-homed nodes, this is if a node has Internet connections to two different segments, it makes it more difficult for an attacker to find a way to split the network [32]. Another method is the Intelligent Neighbor Selection; here, the more nodes that connect to nodes in different segments, the more communications the attacker needs to control [177]. Network Statistics Monitoring is another technique, here, an attacker's rerouting and monitoring are likely to increase network latency, monitoring for this could detect attacks. Finally, Encrypted Authenticated Communications, this ensure that an attacker cannot monitor and change the communications occurring between nodes [32].

#### Sybil attacks

A Sybil attack occurs when an attacker creates many accounts on the blockchain network [328]. This can be useful in eclipse attacks, routing attacks, and attacking Proof of Stake. To perform a Sybil attack, an attacker only needs the ability to create and operate a large number of blockchain accounts [328]. Botnets, virtualization technology, or malware can be used to accomplished this. The best way to protect against a Sybil attack is to use a permissioned or private blockchain where access controls limit the attacker's ability to create accounts on the blockchain [177].

### 2.9.2 System-level vulnerabilities and attacks

#### The bitcoin hack

Bitcoin is designed as a cryptocurrency, which means that it must be validated if transaction amounts are less than the amount of value in the sender's wallet [177]. This transaction validation code included an integer overflow vulnerability that allowed huge transaction amounts to pass the check. An attacker exploited this vulnerability by creating a transaction that sent 184 billion Bitcoin to an account controlled by an attacker.

This would allow the attacker to control over 98 percent of all Bitcoin that would ever exist and would destroy the value of Bitcoin [177]. The Bitcoin network decided to roll back the blockchain to erase the attack [177]. This was an important decision, as the distributed ledger is designed to be immutable but was necessary to preserve the value of the cryptocurrency. The attack showed the importance of performing comprehensive security testing of blockchain code before deployment. An integer overflow vulnerability is a well-known programming flaw and likely could have been identified as part of a security assessment [177].

### The verge hack

The Verge cryptocurrency is a cryptocurrency that aims to preserve the privacy of its users [177]. It was hacked through the clever combination of some of its built-in features, flexible timestamps, and difficulty with updates. The attack caused Verge to create blocks quickly and lose money [177]. This manipulation raised blockchain integrity and security worries, lowering market confidence. After patching the flaws, Verge developers tightened block time stamp restrictions and adjusted the difficulty algorithm to prevent further exploitation.

For secure and private cryptocurrencies, blockchain protocols must be strong and durable, as shown by the Verge hack. Continuous security audits and quick vulnerability responses are needed to maintain confidence and integrity. This incident warns the bitcoin community to be attentive and aggressive about security [177].

### The EOS vulnerability

EOS is an open-source smart contract platform. As a smart contract platform, EOS software needs to be able to parse and execute smart contract files [177]. A buffer out of bounds writing vulnerability in the parsing function allowed malicious smart contracts to exploit the EOS blockchain software. Researchers at Qihoo 360 identified and reported the bug to the EOS developers [220]. Their proof of concept demonstrated that they could bypass Address Space Layout Randomization (ASLR) and obtain a remote shell from the attacked node. As a result, they could completely compromise

the blockchain network and all nodes running it [177].

#### The lisk vulnerability

Lisk is a cryptocurrency that is vulnerable to an exploit taking advantage of two built-in features [177]. Lisk uses the last 64 bits of the SHA-256 hash of a user's public key as their address on the blockchain. This address is not tied to a specific public key on the blockchain until the user performs a transaction either sending cryptocurrency or voting for a delegate [177]. This system can be attacked because transactions sending value to an account do not tie an address to a public key. Accounts that have only received value remain unclaimed.

### 2.9.3 Smart contract vulnerabilities and attacks

#### Reentrancy

A smart contract may be vulnerable to a reentrancy attack if it updates state after performing a state-changing operation [177]. If a smart contract's withdraw function sends value to another smart contract, the recipient smart contract's payable fallback function is called, which can re-call the original smart contract's withdraw function and perform a second withdraw before the user's account balance is updated in the original smart contract [177].

```
1 function withdraw(uint _amount) {
2     require(balances[msg.sender] >= amount);
3     msg.sender.call.value(_amount)();
4     balances[msg.sender] -= _amount;
5 }
```

Figure 2.11: Example of Reentrancy Attack

The sample code in Figure 2.11 is vulnerable to a reentry attack. In line 3, a smart contract fallback function can be called, which can call this function again. Since the smart contract has not yet updated its account balances (performed in line 4), the user can end up withdrawing twice the original amount. The famous breach of the Ethereum DAO smart contract involved exploiting a reentrancy vulnerability. The

smart contract included code similar to the example above, allowing a malicious smart contract to drain value from the DAO smart contract [177].

### Access control

Smart contracts often give different levels of permission to their owners versus other users [177]. If the access control code of a smart contract is improperly implemented, a malicious user can gain control of the smart contract. The snippet in Figure 2.12 is designed to give ownership permissions to the creator of the smart contract as part of the initialization process. However, the code does not check if the initContract function has already been called, allowing any user to call it again and claim ownership of the contract. The Parity wallet was a commonly-used smart contract-based cryptocurrency wallet. It included an initWallet function that stored the list of users authorized to make transactions using the wallet [177]. However, it did not include a check if initWallet had been called in the past, allowing an attacker to call the function for several valuable wallets and claim the cryptocurrency stored within.

```
1 function initContract() public {
2     owner = msg.sender;
3 }
```

Figure 2.12: Example of Access Control Attack

### Denial of service

Denial of Service vulnerabilities make it possible for a smart contract to be rendered non-functional [177]. Two common DoS vulnerabilities are created by poor access control and the potential for infinite loops or recursion.

The code sample Figure 2.13 shows smart contract code that is vulnerable to a Denial of Service attack. If largestWinner is set high enough, the smart contract will require a large amount of gas to execute the selectNextWinners function. Ethereum has a built-in maximum gas limit, meaning that the function could be impossible to run if largestWinner becomes too large.

```
1 function selectNextWinners(uint256 _largestWinner) {
2     for (uint256 i = 0; i < largestWinner; i++) {
3         // heavy code
4     }
5     largestWinner = _largestWinner;
6 }
```

Figure 2.13: Example of Denial of Service Attack

## 2.10 Smart Contracts and Digital Signatures

Smart contracts and digital signatures are the main technologies that support blockchain systems, thus they are the primary drivers for secure, automated and verifiable interactions, without the need for intermediaries. Smart contracts are programs that are self-executing on the blockchain and they automatically execute the agreement terms if the predefined conditions are fulfilled. Digital signatures complement this by supplying a cryptographic way for the verification of the authenticity and integrity of the messages or transactions, as they guarantee that only authorized parties can keep the operations or approve actions on the blockchain. In combination these technologies not only improve the transparency and efficiency of decentralized applications.

### 2.10.1 Smart Contracts

Smart contracts on blockchain technology offer significant potential for enhancing human resources management processes, particularly in payroll and employment systems. These contracts can automate and streamline various HR operations, including employee onboarding, verification, and compensation [216]. They automatically reject duplicate records or incomplete validation data, ensuring data integrity in various domains. For instance, Estonia uses smart contracts and signatures to validate the integrity and authenticity of identity documents and public registry data, which could be extended to verify employee records in a payroll system [202]. In addition, IBM's blockchain solution for contractor labour uses smart contract logic to enforce business rules (e.g. contractors' hours do not exceed purchase order, invoices validated automatically from approved time sheets), which is analogous to enforcing payroll or salary

payments contingent on verified work [94]. Beyond HR, in automated vehicle incident investigations, smart contracts can validate and secure real-time data from multiple sources, enhancing the accuracy of accident reconstructions [75]. In addition, smart contracts are poised to revolutionize auditing practices, enabling real-time, transparent, and immutable logging of transactions [343].

### 2.10.2 Digital Signatures

Digital signatures, based on asymmetric cryptography [115], play a critical role in blockchain-based payroll systems. They authenticate the identity of users who submit or approve transactions, ensuring only authorised HR officers or validators can add or change records. They also guarantee data integrity: any modification after signing is easily detectable, preserving the reliability of payroll data. In addition, digital signatures provide non-repudiation, meaning signers cannot later deny having submitted or approved a transaction [233]. Beyond these core benefits, digital signatures support multi-layer approval workflows, enable integration with existing HR identity management systems, and create secure, verifiable audit trails accessible to both internal auditors and external regulators [226]. Equally, digital signatures create secure, auditable trails accessible to both internal and external parties, providing electronic evidence for compliance and auditing purposes [226].

#### Conclusion

This expanded functionality makes digital signatures a foundational security mechanism in modern blockchain systems, as shown in both technical and applied research [92] [444]. Together, smart contracts and digital signatures strengthen trust, automate processes, and ensure data authenticity within blockchain-based payroll systems.

## 2.11 Applications of blockchain

Blockchain applications have moved beyond cryptocurrency. The technology is used in various sectors due to its transparency and efficiency. Kuhn et al. designed a de-

centralized blockchain application called TokenTrail. It focuses on traceability requirements of multi-hierarchical assembly structures [211]. The architecture was based on an Ethereum consortium network that ensures a trusted and shared database within an economic processing framework. The framework addresses risks identified for conventional systems and as cost and data risks arising from the interference of intermediaries. While Antwi et al. created testing scenarios using Hyperledger Fabric to study different criteria and use cases for healthcare applications [30]. They evaluated the representative test case scenarios to assess the blockchain-enabled security. R3 is an enterprise software company that leverages on blockchain technology to enhance business enterprise. It ensures that business transactions are managed among peers concerned without exposing them to other participants in the network. It accommodates more than 200 firms, most of which are banks [74].

In addition, Lyu et al. designed and proposed a Secure Blockchain-based Access Control (SBAC) framework context provider that can share, audit and revoke its contents securely [234]. Also, F. Chen et al. proposed a framework to assist inexperienced users in choosing appropriate strategies where different application scenarios are concerned. The authors demonstrated the practicality of the proposed framework through a series of experiments as well as a real-world case study. Well-known companies such as Microsoft, IBM, and Oracle utilize the benefits of blockchain technology [353].

## 2.12 Blockchain adoption

Blockchain is adopted and used in many developed and developing countries. Georgia, a country in Europe, was the first to store land tiles on the blockchain platform. The country's land registry has been using blockchain since 2016. In 2017, the project was extended to accommodate land services such as mortgages, new title deeds, and sales [365]. Similarly, Dubai also runs its land registry on blockchain. The government recorded 56 000 transactions on blockchain with a total value of Dhs 228.5 billion in 2018, ranking the city 10th position globally for property registration [120]. On the other hand, Honduras' government also built a similar blockchain land registry but

it did not succeed due to rigidity and inflexibility with their present non-digital land record system [340].

Estonia is another country that has been using blockchain for more than a decade. In early 2017, the government transferred one million of its citizens' records to blockchain [214]. The country later expanded its use of blockchain to cover security, legislative, health, and other registries. The Estonian Guardtime (Estonian Government Owned Software Company) developed a keyless Signature Infrastructure (KSI) to protect the network against threats. In view of this, the American government paid Estonia and Galois 1.8 billion dollars to study and verify the KSI system [117]. Singapore's government uses blockchain to protect bank and invoice fraud [242]. The algorithm of the technology can reject duplicated invoices issued by customers. Before the implementation of blockchain technology, the sum of 200 million dollars was defrauded through duplication of invoices [242].

The UK Department for Work and Pensions ran a blockchain pilot trial to enable beneficiaries to claim, receive and spend their payment benefits on blockchain mobile app tracking system [132]. If the trial is successful, the government will include tax collection and sharing of health records in the system. In 2018, the president of Venezuela launched a digital currency (Petro) that runs on blockchain. Petro, as a national currency, was aimed at strengthening the country's financial security and stability [170].

Illinois explored blockchain to enhance public services and reduce bureaucracy [286]. The technology allows for the conversion of traditional paper certificates into digital formats, with cryptographic hash functions ensuring data integrity [372].

In the same vein, blockchain technology has been explored in Andhra Pradesh, India, for managing land records and improving welfare scheme disbursements. The integration of blockchain with Aadhaar-based identity systems aims to enhance transparency, reduce corruption, and eliminate ghost beneficiaries [305] [190]. Moreso, the UN used blockchain to track aid distribution and ensure only registered and verified individuals received benefits [40]. This application used decentralised identity verification and conditional disbursement through smart contracts; concepts applicable to public salary disbursement and employee validation [40].

Several studies propose blockchain-based systems for secure storage and validation of academic credentials [267] [266] [380] [250]. These systems typically involve storing encrypted certificate data or unique identifiers on the blockchain, ensuring immutability and easy verification [267] [380]. Some approaches incorporate cloud storage to reduce costs associated with blockchain data storage [266]. The use of blockchain for credential verification can significantly reduce verification time, eliminate intermediaries, and enhance trust in the hiring process [250].

Tens of other countries are using blockchain technology such as Russia, Canada, Mexico, China, Sweden, India, and Japan [352].

# Chapter 3

# Theoretical Framework

## 3.1 Introduction

This chapter presents the theoretical frameworks underpinning the study of ghost worker fraud and the adoption of blockchain-based systems in the public sector. The frameworks are grouped into two major categories: fraud-related theories and technology adoption models. Each theory is critically examined for its relevance, strengths, limitations, and applicability to the research problem of reducing ghost worker fraud. Emphasis is placed on selecting the most appropriate frameworks to guide the research design, data collection, and analysis. The chapter concludes by justifying the selected frameworks and summarizing their integration into the study.

The frameworks included in this study were identified through a systematic review of peer-reviewed journal articles, conference proceedings, and seminar books in the fields of fraud management, information systems, and technology adoption. A systematic analysis was conducted across four major academic databases: Scopus, Web of Science, IEEE Xplore, and Google Scholar. The following search terms were employed "fraud theory", "fraud framework", "fraud models", "public sector", and "government employment". Also other keywords were "fraud detection", "employment integrity", "technology acceptance", "UTAUT", "TPB", and "public sector information systems". These keywords were selected to capture both fraud-related theoretical technology acceptance models relevant to employment integrity and adoption in the public sector. The initial pool of theories was then narrowed down by assessing their frequency of use in related studies, their explanatory power, and their applicability to the Nigerian public sector context. The frameworks reviewed include the Fraud Triangle, Fraud Pentagon, UTAUT, and opportunity theory. Others include the diffusion of innova-

tion, fraud management theory, etc. The chapter concludes by justifying the selected frameworks and summarizing their integration into the study.

## 3.2 Fraud-Related Theoretical Frameworks

### 3.2.1 Fraud Triangle Theory

The Fraud Triangle Theory was developed by Donald Cressey, a criminologist, in 1950 after studying the reasons why public office holders commit frauds [31]. Cressey presents three conditions necessary for fraud which include pressure, opportunity, and rationalization [358]. The conditions are discussed with respect to how they can contribute to a deeper understanding of the occurrence of ghost workers in Nigeria. Individuals in a trusted financial position who have financial problems and are aware that they can secretly violate their position to solve their problems will commit fraud [358] because there is a strong relationship between the opportunity to commit fraud and the capacity to conceal fraud [414].

Kohler asserts that the Fraud Triangle Theory could be used to analyze organizational structures, making it specifically applicable to the ghost worker problem [209]. The theory was used in different countries and different contexts to illustrate the risk of corruption and fraud in the public sector [287]. Riney explained the rationale behind why a person commits a corrupt and fraudulent act [335]. He asserts that the fraud triangle theory was established as a means for preventing and detecting fraud.

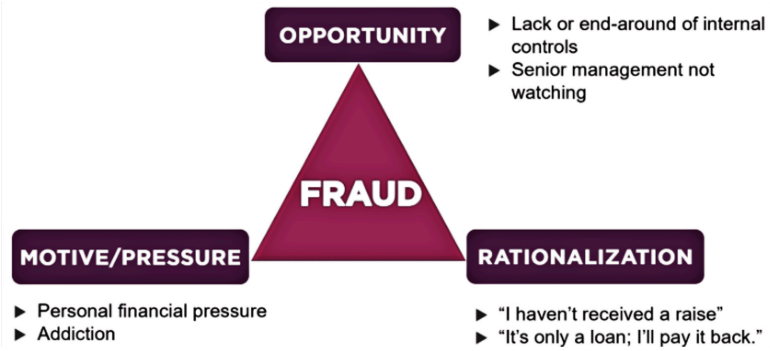


Figure 3.1: The Fraud Triangle Theory
Source: The Fraud Triangle: Three Conditions That Increase The Risk Of Fraud [208]

### Pressure

Cressey viewed that pressure could be as a result of financial, non-financial, political, or social issues such as lavish living and/or lack of financial discipline. Government officials and top managers always want to maintain prominence and, as such, often engage in financial fraud [201]. Emotional pressure could be a result of political ambition or a target to reach some sort of aim, in Nigeria most politicians promise jobs for their people and there are always limited slots. Pressure could be either financial or emotional. Financial pressure is concerned with financial needs [287], for instance, Nigeria's minimum wage is thirty thousand Naira monthly, which is equivalent to thirty GBP, even though the Nigeria Labour Congress (NLC) is struggling hard for the government to review the figure. They embarked on industrial action on 3 June 2024 for the purpose [276], this leads to financial pressure that encourages fraudulent acts. An individual's desire to improve his economic and social status is an example of pressure that could be emotional, financial, or both, and that is the individual's perception of prestige. Another example is, an individual who is responsible for employment process may be inclined to generate ghost worker entries in order to obtain additional funds to satisfy familial obligations or pay personal debts.

Identifying the reasons why employees may resort to fraud is facilitated by comprehending these pressures. These limitations can be alleviated through the implementation of measures such as enhanced financial support systems, employee assistance programs, and the promotion of awareness regarding the repercussions of fraud.

### Opportunity

The opportunity for fraud can occur when institutions and policies are weak and also when there is an ineffective employment and payroll system. In such occasions, the supposed net benefit of committing fraud may be more than the supposed net loss of punishment [224]. Rabi'u et al. affirm that perceived opportunities for fraud are the result of weak internal control structures, poor management oversight, or weak supervision systems on which bureaucrats rely [320]. This weak internal controls, inadequate

supervision, and deficiencies in the verification processes create opportunities for fraud. For example, an official could effortlessly incorporate fictitious employees (ghost workers) into the employment process if there is a lack of a robust system for verifying the existence and employment of employees.

**Rationalization**

This refers to the ability of the fraudster to justify or support their fraudulent activity [287]. Rationalization is seen as the discrepancy between individual belief and cultural value and is taken as a solution to a problem rather than as a problem [351]. In some countries, according to Hechanova et al. rationalization influences how employees perceive fraud [169]. Low wages may also make employees rationalize fraud as a course of compensation [224]. In addition, there are other theories like the Organizational Theory and Bureaucratic Corruption, the Organizational Theory explains how corruption is rationalized, and socialized and get inserted into processes within an organization [37]. While the Bureaucratic Corruption theory focuses on the incentive role that encourages a person when committing a fraudulent act [446]. In the IPPIS context, fraudsters often justify their actions to themselves. A government employee may rationalize "I am underpaid for the volume of work I perform" or "If everyone else is doing it, why should I not?" This rationalization facilitates their justification for participating in fraudulent activities. This study can be used to develop educational programs that emphasize the long-term repercussions of fraud and encourage ethical behavior by understanding common rationalizations. Developing a culture of integrity within government agencies can mitigate the prevalence of such rationalizations.

While the Fraud Triangle is foundational, it has been criticized for oversimplifying the dynamics of fraud. It omits factors such as individual capabilities, organizational culture, and group dynamics. Nevertheless, its focus on "opportunity" makes it particularly relevant to the structural vulnerabilities in Nigeria's centralized payroll and employment system, where inadequate controls facilitate ghost worker fraud.

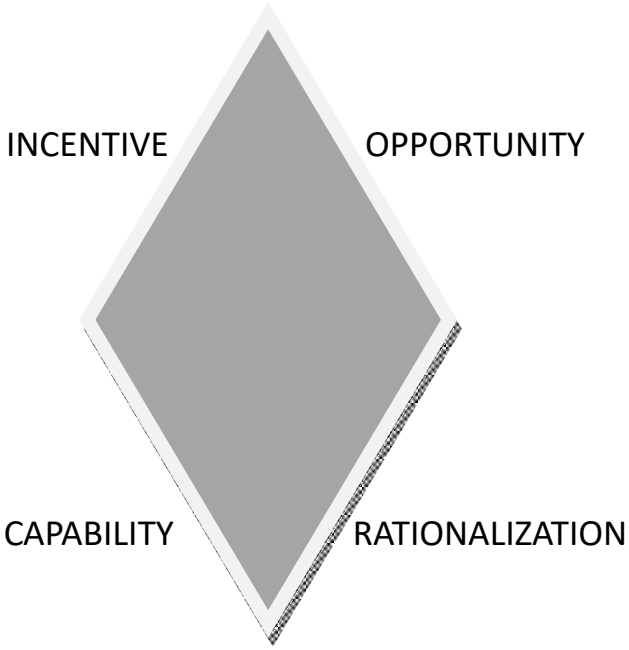


Figure 3.2: The Fraud Diamond Theory
Source: The Fraud Diamond: Considering the four elements of fraud [428]

### 3.2.2 Fraud Diamond Theory

Wolfe and Hermanson modified the fraud triangle theory to add a fourth condition, advancing it to the fraud diamond theory [428]. The fourth condition is the individual's ability to commit fraud. Noting that an individual must be placed in an organization where they can have the authority over whether fraud occurs or not. They must possess the character and abilities to make fraud a reality. Wolfe and Hermanson affirm that it is impossible for most frauds to happen without the right individual with the correct ability. In addition, the right individual must observe and take advantage of opportunity to commit the crime, believing that incentive and rationalization will have to play its role. Moreover, the individual must acquire the capability to identify the chance as an opportunity and to take advantage by stepping in, possibly, multiple times.

#### Capability

Capability denotes the individual's skill set to perpetrate fraud, which includes the knowledge, confidence, and resourcefulness necessary to exploit vulnerabilities [428]. This includes personal attributes such as intellect and creativity, as well as positions of authority and expertise, which allow the individual to effectively execute and conceal fraudulent activities. Conversely, Opportunity refers to the external environment or circumstances that facilitate fraud. It encompasses the existence of exploitable gaps within the system that can be manipulated without immediate detection, a lack of supervision, and weak internal controls. Opportunity pertains to the circumstances that facilitate fraud, whereas capability pertains to the individual's inherent capacity to capitalize on those circumstances.

In the context of this study, the ability to commit fraud necessitates the possession of the requisite knowledge, position, and skills. In the event of ghost worker fraud, an official in a position of authority who has knowledge of the vulnerabilities of payroll systems and has access to them would be able to perpetrate the fraud. The implementation of a blockchain framework not only restricts opportunities, but also necessitates a high level of technical proficiency to circumvent, thereby increasing the barrier for potential fraudsters. Ensuring that no individual has the ability to commit fraud can be achieved through regular training and re-assessment of employee roles.

Although the theory enhances fraud profiling, it introduces abstract constructs that are challenging to measure empirically. This complexity limits its practical application in system-level studies like DEIFP, where emphasis lies on institutional, not personal, enablers of fraud.

### 3.2.3 Fraud Pentagon Theory

The Fraud Pentagon Theory that was developed by Crowe Howart in 2011 builds upon earlier frameworks such as the Fraud Triangle and Fraud Diamond by adding two critical elements which are arrogance and competence [367]. Arrogance reflects an offender's sense of superiority or entitlement that leads them to believe they are above

rules or oversight, and competence, represents the individual's technical knowledge and expertise used to exploit system weaknesses. This makes it a more nuanced tool for understanding insider threats like ghost worker fraud. This theory has been used to identify fake financial reporting in a variety of settings, including Indonesian capital markets and state-owned enterprises [112]. External pressure, insufficient monitoring, and director changes have all been linked to fraudulent reporting, according to studies [318]. Some factors such as pressure and rationalization have been found to significantly predict fraud, arrogance and competence are factors in the fraud pentagon theory that influence fraud [374]. While some of the strengths of the theory include comprehensive behavioural insight and versatility, its limitation could be its complexity and limited empirical validation [98].

While offering depth, the theory suffers from limited empirical validation and applicability to administrative fraud at operational levels. It is less effective in public sector payroll scenarios involving collusive or opportunistic misconduct. This is because such fraudulent activities typically transcend individual behavioural factors and instead emerge from collective actions embedded within organisational structures. In these contexts, ghost worker schemes often rely on the coordinated participation or tacit approval of multiple actors such as payroll officers, human resource personnel, and supervisory officials who exploit systemic weaknesses and administrative loopholes for mutual benefit.

### 3.2.4 Fraud Hexagon Theory

Vousinas introduced the Fraud Hexagon Theory, an extension of earlier fraud models in 2019 [13]. He enhances the model by introducing the S.C.O.R.E. concept that incorporates six key factors: stimulus (pressure), capability, opportunity, rationalization, ego (arrogance), and collusion [415]. The theory offers a comprehensive framework for understanding and detecting financial statement fraud [367]. The concept has six main components: pressure, opportunity, rationalisation, competence/capability, arrogance/ego, and collusion [441] [367]. Recent research have extended this idea to a variety of industries, including banking, manufacturing, and infrastructure [367]. Ghost

worker fraud, where fictitious employees are added to payroll to unlawfully collect wages is a prevalent issue that can be analyzed using this theory. Empirical research indicates that external pressure, opportunity, and collusion have considerable positive effects on fraudulent financial reporting. The model's strengths lie in its capacity to offer a sophisticated framework for risk assessment and function as a diagnostic tool for regulators and auditors, especially in politically sensitive industries [166].
Critical Evaluation: Although conceptually rich, its added complexity and overlap with existing constructs (like opportunity and capability) reduce its distinctiveness. More so, limitations include a lack of attention to behavioural and cultural factors, as well as industry-specific concerns [367]. Also, for a focused study on payroll fraud in public administration, the incremental value it offers over the Fraud Triangle and Opportunity Theory is marginal.

### 3.2.5 Opportunity Theory

In the field of criminology, Opportunity Theory concentrates on situational factors that encourage criminal behaviour, with a particular emphasis on the availability of criminal opportunities and the inadequacy of controls [423]. This approach uses economic market theory to forecast the behaviour of future offenders and victims, emphasizing their interaction [96]. The theory asserts that crime is initiated when motivated offenders encounter suitable targets that lack capable guardianship [332]. It has been implemented in a variety of settings, such as neighborhood-level crime, high-crime areas, and individual victimisation [424].

Researchers have also suggested dynamic, multicontextual approaches to criminal opportunity theory that take into account both human and environmental influences across time [102]. The theory has been modified to account for cybercrimes in the digital age, using the idea of "lagged" interactions between perpetrators and targets in virtual environments [333]. In recent decades, the situational approach to crime has gained considerable prominence in criminology. This theory was initially popularised by criminologists [95], which posited that crime frequently arises from routine activities and social interactions. In this context, opportunity is regarded as a critical factor in the

perpetration of crime. Cohen and Felson argued that criminal incidents are influenced not only by the attributes of the offender or the victim but also by the opportunities presented by the social environment and the organization of daily life [95]. Factors involving opportunity theory includes:

### Routine Activities

Cohen and Felson's theory states that crime occurs when motivated offenders, suitable targets, and a lack of capable guardians converge in time and space [70]. This environmental approach stresses how everyday activities and societal situations influence criminal possibilities [135]. The theory proposes that crime prevention can be done by managing these characteristics, such as diverting potential offenders from suitable targets and improving natural surveillance [135]. While the theory largely focuses on opportunity and situational factors, other scholars argue for its integration with subcultural approaches to better explain violent encounters [205].

### Lack of capable guardianship

Capable guardianship, a core idea in routine activities theory, plays a critical role in crime prevention. Reynald identified three critical aspects of capable guardianship: willingness to supervise, ability to detect potential offenders, and willingness to intervene [332]. Hollis et al. conducted a theoretical reappraisal of guardianship, emphasizing the need for a refined definition that is consistent with its original conceptualisation [173]. Reynald conducted additional research on guardianship using direct measures and primary data collection, emphasizing the importance of observing guardianship in action [332]. Lockitch et al. used guardianship to prevent institutional child sexual abuse, demonstrating how the concept can be applied outside of traditional crime settings.

### Suitable Targets

Crimes are more likely to occur when there is a "suitable target." In fraud cases, the target may be financial systems, organizations, or even individuals who are vulnerable

to exploitation.

**Application to Ghost Worker Fraud** In the context of ghost worker fraud, Opportunity Theory is highly applicable. Public sector payroll systems with weak oversight, poor monitoring, and inadequate cross-checking provide ample opportunity for fraudulent actors to add non-existent employees to the payroll without detection. The lack of capable guardianship such as weak internal controls and insufficient audits allows fraud to continue undetected. Furthermore, the suitable targets in this case are the public sector organizations and their payroll systems, which are vulnerable to manipulation due to lack of effective validation systems.

**Relevance to fraud prevention** Opportunity Theory offers valuable insights for preventing fraud, particularly in organizational settings like the public sector. By identifying and removing opportunities for fraud such as implementing stricter access controls, introducing strong verification systems, and ensuring strong inter-agency checks—organizations can significantly reduce the risk of fraud. Strengthening the guardianship through regular audits, transparency, and oversight further minimizes the opportunities for fraudulent activities to take place [147].

In conclusion, Opportunity Theory underscores the critical importance of the structural and situational aspects of crime, suggesting that reducing opportunities for fraud is a key strategy for preventing criminal behavior. In the case of ghost worker fraud, addressing systemic weaknesses and enhancing oversight can disrupt the opportunities that allow fraud to thrive. This theory directly applies to ghost worker fraud, where institutional lapses such as weak inter-agency validation and absence of cross-checks provide opportunities for exploitation. It complements the Fraud Triangle by expanding its focus on systemic risk factors.

### 3.2.6 Institutional Theory

The study of institutional theory looks at how normative pressures affect organizations and cause them to embrace elements that are accepted as legitimate and boost their

chances of surviving [447]. According to this idea, organizational structures frequently serve as myths that offer stability and legitimacy by reflecting rationalised institutional rules [246]. An institutional perspective is used to examine the idea of moral collapse in organizations, highlighting the interdependence of people, organizations, and moral communities [362].

Institutional logics are internalised as associative networks of schemas at the individual level, influencing behaviour through a process known as institutional frame switching. Experiments have shown that implicit theories, a crucial schema connected with institutional logics, can influence individual behaviour [150]. Together, these investigations shed light on the intricate relationship between institutional frameworks and human conduct, offering insights into both organizational dynamics and pervasive misconduct. Fundamentally, Institutional Theory asserts that organizations are social institutions influenced by shared norms and practices rather than merely being groups of individuals. Members of an organization are governed by these institutionalised norms, which either encourage moral behaviour or allow immoral behaviour. Even if these norms support or facilitate fraud, they may eventually become so deeply rooted that they are accepted as the usual.

## 3.3 Technology Adoption Frameworks

### 3.3.1 Diffusion of innovation theory

Gabriel Tarde, a French sociologist first discussed the Diffusion of Innovation (DoI) Theory in 1903 and plotted the original S-shaped diffusion curve as shown in Figure 3.3 [394]. Ryan and Gross then introduced the adopter categories that were later used in the current theory made popular by Everett Rogers [345]. Based on Tarde's work, Ryan and Gross developed adopter categories in their 1943 research on hybrid seed corn acceptance among farmers [345]. In the DoI Theory, Everett Rogers popularised innovators, early adopters, early majority, late majority, and laggards. Rogers' work detailed adopter categories and social factors affecting diffusion, refining the theory. Due to their curiosity and risk-taking, innovators adopt new ideas first. Early

adopters, often opinion leaders, legitimise the innovation. The majority of adopters are early and late majority, swayed by peer pressure and perceived innovative benefits. Slow adopters, usually sceptical or without resources, are the last. This sophisticated approach helps explain how innovations spread and gives strategic insights for supporting new technologies like blockchain solutions in employment systems.

The DoI concept is often accepted as an effective change model for managing technological innovation, where the invention itself is altered and presented in ways that satisfy the needs of all levels of users. It also emphasizes the value of networking among peers and communication during the adoption phase [203]. DoI is the process through which individuals take up a novel concept, service, behavior, ideology, etc. Rogers described this procedure and emphasized that, in most circumstances, the first few people to adopt the new thought are receptive to it. A critical mass develops as more and more individuals become receptive to it as these early innovators "spread the word." The new concept or product gradually spreads throughout the populace until a saturation limit is reached [199].

The S-curve as shown in Figure 3.3 is currently a fairly logical model for how innovations and other technologies spread among a population. The model basically demonstrates that any invention is initially accepted by a small number of individuals (or organizations). As more people use it, more people notice it being used, and if the invention is better than what came before, more people start using it. When the diffusion reaches a critical mass, it progresses quickly [82].

Diffusion of innovation has been used by many scholars in many different ways, Agi and Jha developed a comprehensive framework for blockchain adoption in supply chain industries by the use of enablers and empirically assessing their interdependencies on adoption [10]. The enablers were picked using literature review from the lenses of DoI. They discovered that the relative benefit of the technology and outside pressure are the two most important kinds of enablers that influence the adoption of blockchain in the supply chain. The analysis also demonstrates the crucial causal relationships between consumer interest in traceability data, the formation of a legislative framework for blockchain usage, and acceptance of blockchain technology's promise to lower

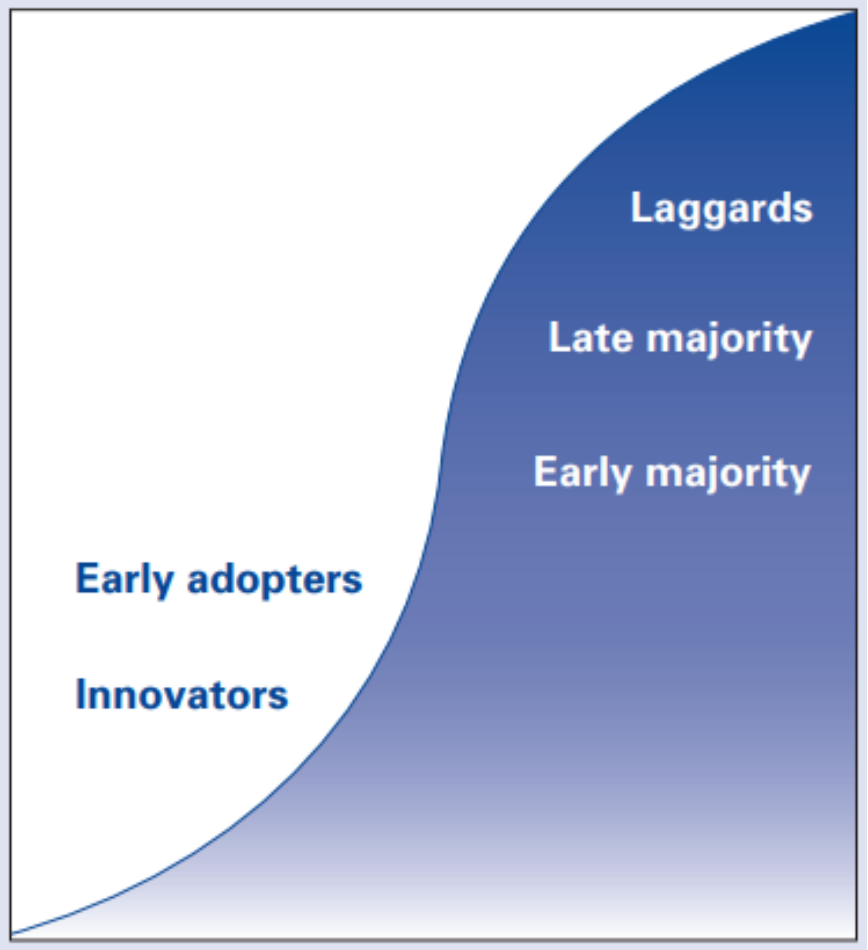


Figure 3.3: The Diffusion S-Curve [82]

transaction costs.

While Goh and Sigala examines the factors that stop university teachers from using modern Information and Communication Technologies (ICT) in their academic practices and discusses solutions to these problems [153]. The study uses literature review to analyze issues related to ICT integration in schools using the DoI theory as a theoretical lens to better understand educational change. The study provided instructional guidance and inspiration for academics on how to incorporate ICTs into their classroom practices. In addition, P. Grover et al. explore the blockchain technology diffusion in different industries through a combination of academic literature and Twitter [157]. The academic literature and social media insights have been utilized into group sectors of five stages of the innovation. The findings imply that some sectors are already producing specific blockchain applications.

Furthermore, Semenova examined the adoption process of emerging technology specifically on the blockchain. It was discussed from positions of Technology Acceptance Model (TAM) and DoI [360]. The findings point to a lack of empirical research studies and the necessity for more thorough theory development in order to hasten the adoption process within organizations. Meanwhile, Min et al. examines consumer acceptance of the Uber mobile application through the lenses of the DoI Theory and the TAM [249]. The findings imply that relative advantage, compatibility, complexity, observability, and social influence have a considerable impact on perceived usefulness and perceived ease of use, which in turn affect consumer attitudes and adoption intentions. The two traditional adoption theories are successfully integrated in the study. More so, Ullah et al. proposed blockchain adoption in smart learning environment by integrating DoI and TAM. The idea is to examine the technology adoption models for developing states [401]. The outcomes demonstrated that compatibility significantly affected the utilization of blockchain in smart learning settings.

In another vein, Oyelana et al. examine innovation attributes affecting the adoption of exclusive breastfeeding in Africa using Roger's DoI theory [298]. A comprehensive analysis of the available data on exclusively breastfeeding in Sub-Saharan Africa was done. In accordance with the DoI theory, eligible studies were chosen, and a directed

content analysis technique to data extraction was used to aid narrative synthesis. The main findings show that a number of breastfeeding techniques are in odds with traditional African cultural beliefs and behaviors. Equally, Cain and Mittman studied Diffusion innovation theory for clinical change. The aim is to adopt evidence-based practice in determining healthcare outcomes. They submitted that applying Roger's diffusion model may facilitate the adoption, and it will also provide important insights into why some practices change and some do not [82].

Regarding the understanding of the implementation of blockchain technology within government processes, DOI Theory is particularly pertinent. It has the potential to offer insights on the ways in which blockchain innovations can be introduced and adopted by government employees and institutions. While DOI Theory provides a helpful framework for understanding the adoption process, this study focuses more on the specific motivations and mechanisms underlying fraud (which are covered by the Fraud Diamond Theory) and the acceptance of technology (which is covered by TAM). In light of this, DOI is regarded as a supplementary work to the fundamental objectives. While useful in framing adoption phases, the theory lacks specificity on organizational decision-making or individual acceptance drivers in hierarchical structures. Terms like "laggards" can be ambiguous or culturally insensitive if not contextualized. Hence, it was not selected as a primary framework.

### 3.3.2 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) is regarded as the most significant and frequently used theory for explaining an individual's acceptance of information systems [221]. TAM was first introduced in 1986 by Fred Davies [221]. The model is the most popular theoretical model in the Information Systems (IS) field over time. The theory is based on the Theory of Reasoned Action (TRA) which was used to explain the individual's acceptance of information systems [382]. In the TAM model, an individual's information systems are determined by two factors; Perceived Usefulness (PU) and Perceived Ease of Use (PEU). Davies defined perceived usefulness as the subjective probability of the prospective user that using a specific application system will improve

their job or life performance. Perceived Ease of Use (EOU) is the degree to which the prospective user expects the target system to be free from applying effort [382].

Several studies have been used to test the model and results have been reliable. Y. Lee et al. trace TAM's history, examine its findings from inception, and carefully project where it will go from there [221]. This study used a meta-analysis of 101 articles published between 1986 and 2003 to assess the progress of TAM and the results of TAM research. This research discovered that TAM has continuously advanced over that time and has been elaborated by researchers, addressing its shortcomings, including more theoretical models or introducing new external variables. Similarly, King [206] used 88 published studies that provided sufficient data to statistically meta-analyze TAM in various fields. The findings demonstrate that TAM is a sound model that has been frequently applied and is valid, with the potential for greater applicability. To find out in what circumstances TAM might have varied effects, a moderator study involving user types and usage types was conducted. The study supported the value of substituting students for professionals in some TAM investigations, as well as possibly more broadly. Additionally, it demonstrated the efficacy of meta-analysis as a thorough replacement for qualitative and narrative literature review techniques.

In contrast, Chuttur presented a historical overview of the Technology Acceptance topic (TAM) by reviewing the development of TAM, its main applications, extensions, limits, and criticisms from a chosen list of published works on the topic. Despite the fact that TAM is a model that receives a lot of citations, there are now conflicting views among researchers on its theoretical underpinnings and practical applicability [93].

Deshmukh et al. investigates the factors that influence the adoption of e-learning by sports science education students during Corona Virus Disease 2019 (Covid-19) using a survey of 974 students from five Indonesian Higher Education Institutions (HEI) [379]. The theoretical basis for the study was an enhanced version of the TAM, with facilitating conditions as the external element. The results showed that the TAM-based proposed scale had a successful explanation of the variables influencing the utilization of e-learning by Indonesian sport science students during the Covid-19 pandemic.

More so, Singh et al. presents a framework to examine FinTech adoption and use

from the perspective of the TAM and the other two constructs [371]. A measurement scale was created through iterative discussions with experts. Data was collected from 439 active Internet users and was analyzed using structural equation modeling and multi-group analysis. Part of the discovery was perceived usefulness and social influence are the main factors influencing behavior intention to use fintech services, with social influence having a considerable negative influence. Also, the perception of security among elder users is also strongly influenced by age.

In the same vein, Rafique et al. investigates the adoption of Mobile Library Applications (MLA) using a proposed model that is developed from the TAM [321]. A self-administrated cross-sectional survey was used to collect information from 340 MLA users, and Analysis of Moment Structure (AMOS) was used to analyze the results. The results showed that perceived usefulness and perceived ease of use are directly significant predictors of the intention to use MLA. The discovery can serve as a roadmap for making wise choices when developing and designing MLA. Additionally, the results can be used to guide resource allocation to fulfill the library's vision and goal.

Even though TAM is important in several studies and widely used, in the context of this research, it simply ignores external and some organizational factors.

### 3.3.3 Unified Theory of Acceptance and Use of Technology (UTAUT)

The Unified Theory of Acceptance and Use of Technology (UTAUT) is a model for predicting technology adoption and use [412]. It suggests that performance expectancy, effort expectancy, and social influence predict behavioural intention, whereas enabling conditions and behavioural intention determine use behaviour [388]. A meta-analysis indicates a high relationship between performance expectancy and behavioural intention, but weaker relationships for other components [388]. UTAUT has been widely employed in a variety of domains, including education, where it has been used to investigate learning management systems, mobile learning, and tablet computers [296]. Researchers have proposed model expansions, such as include usability, learnability, and attitude components for educational settings [296]. Ghost worker fraud could be analyzed using this theory. While UTAUT has its advantages, some contend that its

widespread adoption has hindered theoretical advancement in technology acceptance research [412]. UTAUT's robustness and applicability to both public and private sectors make it an ideal fit. It aligns with DEIFP's multi-stakeholder nature and can guide the analysis of adoption intent among government agencies.

### 3.3.4 Unified Theory of Acceptance and Use of Technology (UTAUT) 2

The Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) is an enhanced model that describes user technology adoption by combining eight key technology acceptance models [397]. UTAUT2 adds three more components to the original UTAUT: hedonic motivation, price value, and habit [412]. This extended model explained much more variance in behavioural intention and technology use than the original UTAUT [412]. UTAUT2 can be used in a variety of settings, including virtual learning environments, to uncover factors impacting technology adoption intentions [45]. Individual variations such as age, gender, and experience are considered moderating factors in the model [412]. UTAUT2 has been extensively investigated and expanded since its inception in 2012, with academics applying it to a wide range of technological contexts and organisational settings [397]; [45]. These extensions are not relevant to public sector adoption where user experience and monetary cost are secondary. Thus, UTAUT remains the preferred model.

### 3.3.5 Theory of Planned Behavior (TPB)

The Theory of Planned Behaviour (TPB) is a commonly used social-psychological model for forecasting and understanding human behaviour [187]. It proposes that intentions are motivated by three major factors: attitudes towards the behaviour, subjective norms, and perceived behavioural control [207]. These elements are founded on behavioural, normative, and control views, respectively [207]. The TPB has been widely utilised in information systems research to better understand individual behaviours related to technology adoption [196]. Despite its predictive power and extensive use across fields, some researchers have proposed additional components to improve the

fundamental model [196]. The TPB has also helped design additional frameworks, such as the TAM [196]. Despite numerous criticisms and limits, the theory remains a useful tool for studying human behaviour in a variety of circumstances [196]. TPB provides behavioral insight but lacks the structural elements found in UTAUT. It is better used in conjunction than as a standalone model.

## 3.4 Fraud Management Lifecycle Theory

Fraud Management Lifecycle Theory was proposed by Wilhelm in 2004, he presented eight components that determine success or failure in fraud management [425]. They include Deterrence, Prevention, Detection, Mitigation, Analysis, Policy, Investigation, and Prosecution.

**Deterrence:** This is the first stage and it refers to actions intended to discourage efforts to commit fraud [425].

**Prevention:** This stage involves keeping criminals away from executing fraudulent activities. It entails hindering or preventing fraudsters from perpetrating criminal acts in organizations. It also focuses on implementing protective systems, processes, and procedures that make fraud difficult to commit.

**Detection:** Detection is the third stage of the Fraud Management Lifecycle and it is connected with activities intended to discover and locate fraud before, during, or after it is committed [425].

**Mitigation:** This stage activities are those aimed to lessen the extent and the amount of the related fraud losses. It is a stage for intervention, it may even stop fraud from occurring [425].

**Analysis:** The Analysis stage has two basic functions: identify and understand fraud losses that happen in spite of deterrence, prevention, detection, and mitigation stage

together with monitoring the performance of all the stages of the fraud management lifecycle [26].

**Policy:** Policy activities create, evaluate, communicate, and implement fraud policies to cut down the incidence of fraud, and to assign the resources needed to combat fraud successfully [425].

**Investigation:** Investigation is aimed to collect adequate evidence to prosecute fraudulent activity and to assist in obtaining compensation. Investigation means to run a careful and systematic inquiry by observation and examination of facts [245].

**Prosecution:** This phase is concentrated with undertaking legal or disciplinary action against suspects. The activities at this stage are majorly for the judicial and the law enforcement officers. The three aims of prosecutions are to punish the fraudster to prevent further occurrence. Secondly, prosecution seeks to create, preserve, and develop organizations' reputations and the third goal is to obtain recovery wherever possible [425]. Oguzierem and Joab-Peterside assert that the Fraud Management Lifecycle theory is adaptive and transforming, it reflects all factors and stages necessary to investigate and deter fraud [292]. Information technology is another reason for adopting the theory because it plays an important role during the course of the Fraud Management Lifecycle, and all the stages benefit from the effective application of information technology resources [425]. Figure 3.4 is the linear representation of the fraud management lifecycle theory.

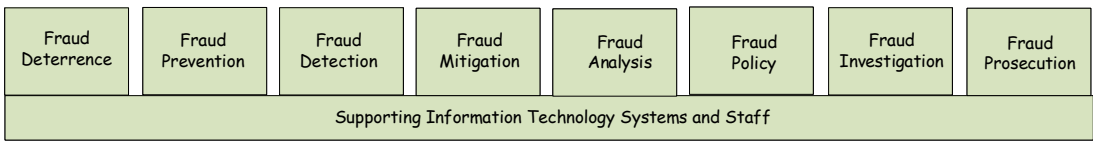


Figure 3.4: The Linear Representation of the Fraud Management Lifecycle [425]

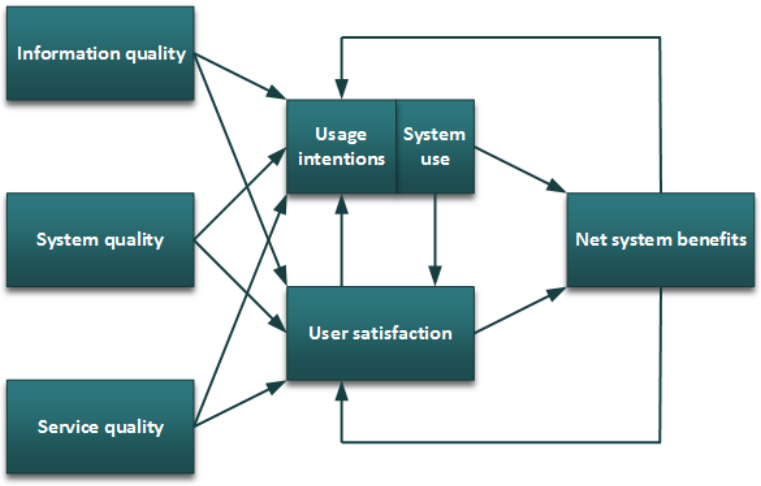


Figure 3.5: The Information System Success Model [426]

## 3.5 Information system success model

The Information System Success Model was proposed and developed by Delone and McLean in 1992 [426]. The model was later reviewed in 2003 based on definitions and corresponding measures and was then classified into major success categories [426]. The updated model consists of six dimensions as shown in Figure 3.5 which include; system quality, information quality, service quality, intention to use, user satisfaction and net benefit. Several researchers have used the model for studies relating to computer and information system performance [426].

**Service quality:** Ramya et al. defined Service Quality as the ability of a service provider to satisfy customer in an efficient manner through which the service provider can better the performance of business [325]. Meanwhile, Petter et al. viewed service quality as a quality of service or support received by system users from Information System organization or IT support unit [312]. This support may include responsiveness, accuracy, reliability, technical competence or empathy.

**System quality:** Freeze et al. considered System Quality as user's perception of a system's performance when the availability of people, hardware and software is put in place [142]. While Petter et al. argued that System Quality is the desirable charac-

teristics of an information system which include ease of use, system flexibility, system reliability, intuitiveness, sophistication and response time [312]. According to Zulfan, system quality is characterized by the desired information system which is used by the users and decision makers [448].

**System use:** William and Ephraim defined system use as degree and manner in which user utilize the capabilities of information system [426]. This may include amount of use, frequency, nature, appropriateness, extend and purpose of use. System use is an important measure of system success.

**User satisfaction:** Freeze et al. viewed user satisfaction as a measure of successful communication among information systems and its users [142]. It is also defined according to Ives et al. 1983 in [142] as the extent to which learners believe the information system meets their needs. However, Petter et al. looked at User satisfaction as user's level of contentment with the information system [312].

**Net benefit:** Petter et al. is of the opinion that Net benefit is concerned with the dimension on which Information System contributes to the success of individuals, groups, organizations, industries and nations [312]. This includes improved decision making, improved productivity, increased sales, cost reduction, improved profits, market efficiency, customer welfare, creation of jobs and economic development. Meanwhile, William and Ephraim say that net benefit as a dimension is one of the components updated by Delone and Mclean in 2003.

## 3.6 Comparative Evaluation and Framework Selection

A comparative analysis of all discussed theories is provided in Table 3.1. The evaluation considers criteria such as empirical validity, relevance to fraud prevention, suitability for public sector contexts, and ease of operationalization. Based on this assessment and in summary, the study adopts the Fraud Triangle, Opportunity Theory, and UTAUT frameworks for the following reasons:

**Fraud Triangle:** Emphasizes motivational and cognitive factors driving fraud.

**Opportunity Theory:** Focuses on structural enablers of fraud, highly applicable to the Nigerian public sector.

**UTAUT:** Provides a holistic view of technology adoption across individuals and institutions.

Table 3.1: Comparative Analysis of Theoretical Frameworks

| **Framework** | **Strengths** | **Weaknesses** | **Applicability to DEIFP** | **Selected?** |
|---|---|---|---|---|
| Fraud Triangle | Simple, well-established, focuses on motivation and opportunity | Omits capability, lacks group dynamics | High: Explains individual fraud behavior in weak control environments | Yes |
| Fraud Diamond | Adds capability; suitable for profiling | Abstract, hard to measure empirically | Moderate: Useful but less applicable at institutional level | No |
| Fraud Pentagon | Psychological insights (arrogance, competence) | Limited empirical use; better for executive fraud | Low: Focuses on top-level fraudsters | No |
| Fraud Hexagon | Includes collusion; broader view | Complex, overlaps with other models | Moderate: Relevant but excessive complexity | No |
| Opportunity Theory | Structural and environmental focus | Doesn't address personal motivations | High: Aligns with DEIFP's design goals | Yes |
| Institutional Theory | Explains adoption via external pressures | Doesn't explain internal processes | Moderate: Good for policy context, not fraud analysis | No |

*Continued on next page*

Table 3.1 – *Continued from previous page*

| **Framework** | **Strengths** | **Weaknesses** | **Applicability to DEIFP** | **Selected?** |
|---|---|---|---|---|
| Diffusion of Innovation | Explains spread of innovation | Lacks organizational detail; generic categories | Low: Limited applicability to DEIFP | No |
| TAM | Widely used, simple | Ignores external & organizational factors | Moderate: Lacks depth for DEIFP | No |
| UTAUT | Comprehensive, organizationally grounded | Requires calibration, complex | High: Fits DEIFP's multi-stakeholder ecosystem | Yes |
| UTAUT2 | Adds consumer elements | Not relevant in public sector | Low: Too focused on consumer tech | No |
| TPB | Strong behavioral insights | Ignores organizational structure | Moderate: Supportive, not sufficient alone | No |

The integration of Fraud Triangle, Opportunity Theory, and UTAUT provides a multifaceted lens through which the research problem is examined. These frameworks inform the design of the DEIFP framework by identifying systemic loopholes that enable fraud (Opportunity Theory), understanding individual motivations (Fraud Triangle) and evaluating stakeholder readiness and resistance to blockchain adoption (UTAUT). These theories also guided the development of data collection instruments and the interpretation of both qualitative and quantitative results.

## 3.7 Summary

This chapter presented a comprehensive and critical review of theoretical frameworks related to fraud and technology adoption. Through comparative analysis, three frameworks; Fraud Triangle, Opportunity Theory, and UTAUT—were selected as most relevant to this study. These frameworks collectively support the analysis of fraud causation and the technological, behavioral, and institutional dynamics shaping the adoption of the DEIFP framework in Nigeria's public sector.

# Chapter 4

# Data analysis of the 2021 survey

The first empirical phase of this research was conducted in 2021 and was focused exclusively on federal government employees as respondents. This phase was designed to supplement the literature review in Chapter 2, which highlighted persistent claims that the IPPIS suffers from transparency challenges and has not been able to fully eliminate ghost worker fraud in the employment process. By directly engaging with employees who interact with IPPIS in practice, this early investigation sought to validate or challenge those claims from the perspective of system users themselves.

## 4.1 Methodology

Research surveys are essential instruments for data collection, particularly in investigations concerning the beliefs, attitudes, and actions of particular groups [71]. The survey method enables us to gather quantitative data directly from individuals who are impacted by or involved in the IPPIS process, thereby offering valuable insights into the system's functionality and vulnerabilities.

### 4.1.1 Research Type

Research Type is structured to clarify the nature, rationale, and methodological orientation of the study. Each type is discussed in relation to its relevance to the research aims and the nature of data collected. It provides a conceptual foundation for understanding where the current study fits within broader research traditions. S. B. Mishra and Alok identified two types of research, namely, Descriptive vs. Analytical, and Applied vs. fundamental [251]. Understanding these research principles helps us comprehend this study's methods and their suitability for answering the research questions and objec-

tives. The following sections will describe the survey methodologies used, why they were chosen, and how they help achieve the study objectives.

### Descriptive vs. analytical

The purpose of descriptive research is to explain a set of circumstances. It consists of different kinds of surveys and fact-finding investigations and centers on answering what, when, where, and how. The purpose of descriptive research is to systematically explain the current phenomena under study. In this kind of research, the researcher will collect the available data through the use questionnaire, interview, or even observation [39]. The key element of descriptive method is, scientists do not have control over the variables established instead just to report events. Atmowardoyo states that the descriptive research covers some types of approaches such as survey, correlation study, qualitative study, or content analysis which may involve either qualitative or quantitative analysis [39]. On the other hand, analytical research involves evaluation of facts and information concerning to the research being carried out. Moreover, in analytical research, facts, data and information already available is always used by the researcher for analysis [39]. This study employs the descriptive research through a survey approach.

### Applied vs. fundamental

According to Atmowardoyo applied research is the process of finding a solution for certain, practical problem confronted by an individual, industry or society [39]. While fundamental research is mainly focused with the formulation of a theory. Fundamental research is concerned with the development of theories while applied research is used to tackle specific issues. Then, applied research is more concerned with practical issues than theoretical research [402]. Hence, this study is focused on the applied research, where practical solution is obtained that could curb ghost worker fraud in Nigeria.

### 4.1.2 Research approach

Research approach refers to the outline to be observed when answering research questions which entails deciding on research objectives, sampling methods, data collecting method, method of data analysis and the type of research design one will adopt [241]. Experts use two different research design approaches which are quantitative and qualitative [39]. Quantitative approach is the research design which involves deductive thinking that determines a hypothesis which in turn supports or rejects a theory. In quantitative approach, organized inquiry of phenomenon is considered through the collection and analyzing of numerical data. Quantitative research design often deploys research method such as experiments, survey, and correlation studies.

On the other hand, qualitative approach is the research design concerning inductive thinking to uncover hypotheses which in turn be developed into a substantive theory. The data under analysis are verbal description poured into ground notes. Qualitative data can be analyzed through steps such as comparison, triangulation, coding, integration, and interpretation. The approach often adopts research method such as ethnography, phenomenology, narrative inquiry, case study, participant observation etc [35]. This study adopts the quantitative approach where questionnaires were administered to collect, analyze, and interpret data because it allows for the objective measurement of perceptions across a large population and facilitates statistical comparison between variables

### 4.1.3 Research purpose

Exploratory, descriptive and explanatory are the three main classifications of research purpose [336]. They define the methods and rules to be used in answering research questions successfully [355]. However, methods are bound to change in the course of research before completion and this implies the altering of a method or the use of additional method.

**Exploratory research:**

This is usually the initial research that leads to a theoretical or hypothetical idea. It entails an individual developing an idea on something and tends to seek more understanding about it. In exploratory research, foundation or groundwork on a certain idea is laid with the intent of it leading to future studies, or a concept observed might be explained by an existing theory [113]. Exploratory research happens when there are only a few or no previous studies [21]. Exploratory research can emerge as either a new topic or a new angle, John Watson an American psychologist began his research on a new topic on human behavior and learning [21]. On the other hand, new angle is when new ways come from looking at other things, either from new way of measuring something or from a theoretical perspective. For example, social media has made the world seen as a little globe. Exploratory research focuses on exploring a particular social phenomenon along with asking questions regarding that phenomenon [195].

**Descriptive research:**

This form of research focuses on systematically describing the characteristics, behaviours, or opinions of a population or phenomenon as it exists in its natural setting [385]. Unlike exploratory research, which seeks to generate new ideas or hypotheses, descriptive research aims to provide an accurate representation of existing conditions or relationships among variables. It answers questions such as “what,” “who,” “where,” and “how often,” without necessarily explaining “why” those conditions occur [385]. According to Swatzell and Jennings, descriptive research enables the collection of quantifiable information that can be statistically analysed to reveal trends, attitudes, or distributions within a given group [385]. Its analysis serves to organize data and tell the story of the sample group, providing a sense of order that enables researchers to understand distributions and characteristics within populations [108]. This methodology has gained popularity due to its flexibility in combining different data collection techniques and its reduced reliance on numerical measurements for variable assessment [143]. Descriptive research does not manipulate variables but instead captures and

summarises realities as they are observed [277, 385]. It often forms the basis for further explanatory or experimental investigations by identifying patterns that warrant deeper analysis. For example, a researcher might use descriptive statistics to measure the prevalence of ghost worker perceptions among government employees, providing foundational evidence for designing anti-fraud interventions. In essence, descriptive research offers a clear snapshot of existing phenomena, making it a crucial step in understanding organisational, social, or behavioural trends before advancing to more complex analytical or causal studies, [8].

**Explanatory research:**

M. Thomas and Pierson viewed that explanatory research attempts to identify causes, establish a connection between factors, and determine impacts on behavior of a social phenomenon, along with predicting how one phenomenon will change or differ in relation to a different variable [392]. The concept focuses more on the source and reasons for occurrence of a problem. Glicken defined explanatory research as a concept that attempts to provide significant and exact conclusions from adequate existing information [151]. It presents evidence that endorses or opposes a concept with an explanation or prediction. The model is not only deductive but quantitative in nature. Explanatory research assists in analyzing patterns and devising hypotheses that predict or guide future endeavors. It also helps individuals understand and establish relationships between variables [148]. This research will use exploratory, descriptive and explanatory methods as it focuses on a well-defined socio-behavioral theory that applies to the use of questionnaires to acquire data on IPPIS ghost worker fraud.

### 4.1.4 Method of data collection

Data collection is a major stage in research that enables the researcher to discover answers to research questions [387]. Taherdoost defined data collection as the process of gathering data with the purpose of gaining insights concerning the research topic [387]. Generally, the two main categories of data collection methods are Primary Data Collection and Secondary Data Collection. Primary data collection refers to the process

of gathering data through interviews, surveys, or experiments [43].

On the other hand, secondary data collection is data collected by someone rather than the main researcher, for example, books, newspapers, magazines, journals, etc. Primary data can be obtained by researchers either by interviewer-administered questionnaires or self-administered questionnaires for their research. While respondents fill out the self-administered questionnaires, interviewer-administered questionnaires are logged in accordance with the respondents' answers [254]. In this research, primary data was gathered from employees of the Federal Government of Nigeria with the intent of assessing employees' perceptions of how IPPIS influences ghost workers in Nigeria and how the DEIFP is perceived. Self-administered questionnaire was adopted as the major data-gathering tool. This is because it allows the collection of data from a larger audience in a timely manner, which is considered a key advantage [355].

Moreover, Vaus viewed that self-administered questionnaires give room for anonymity and encourage honest, quick, and easy responses [411]. Also, anonymous surveys reduce social bias and make respondents confident in expressing their views [155]. This study adopts the quantitative approach where questionnaires were administered to collect, analyze and interpret data as presented in Data analysis of the 2021 survey and Data analysis of the 2024 survey. The study also used the qualitative method with secondary data where some ghost worker fraud-related cases were gathered and analyzed as presented in Evaluation by case study.

### Recruitment of Participants

Participants for the 2021 survey were exclusively federal government employees enrolled on the IPPIS platform. Recruitment was conducted primarily through digital outreach, leveraging WhatsApp groups commonly used for departmental communication within ministries, departments, and agencies. This approach enabled rapid distribution of the survey link to a broad pool of potential respondents. In addition, direct phone calls were made to selected employees to encourage participation and ensure adequate representation across different government institutions.

### Participants' Briefing

Before completing the questionnaire, participants were provided with a structured briefing embedded in the Participant Information Sheet (PIS) (see Appendix C). The PIS outlined the purpose of the study, its background, and the objectives of the survey. It also explained the confidentiality of responses and the voluntary nature of participation. This briefing ensured that respondents understood the context of the research and the relevance of their input in evaluating IPPIS's effectiveness in addressing ghost worker fraud.

### Replicability and Response Rate

To enhance replicability, detailed records of recruitment and participation were maintained. A total of 145 responses were received, out of which 144 were valid for analysis. All respondents were federal government employees, reflecting the public sector orientation of the study. The documentation of sampling criteria and distribution methods provides transparency for future researchers seeking to replicate or build upon this work.

### Inclusion of Supporting Documentation

To strengthen transparency and replicability, the following documents are included as appendices: the 2021 Ethics Application (Appendix A), the 2021 Ethics Approval Email (Appendix B), the 2021 Participant Information Sheet (Appendix C), and the Consent Form (Appendix D).

## 4.2 Survey Design

The 2021 survey adopted a structured questionnaire as the primary instrument for quantitative data collection, aimed at capturing federal government employees' perceptions of the Integrated Personnel and Payroll Information System (IPPIS) in Nigeria [16]. The design was informed by the literature reviewed in Chapter 2, which highlighted persistent issues of transparency, integrity, and ghost worker fraud within IPPIS.

The questionnaire consisted exclusively of closed-ended questions to enhance ease of response and improve participation rates [110]. Items were derived from a comprehensive review of literature on payroll systems and employment fraud, including works such as [39, 138, 180, 351, 440]. The objective was to capture all relevant factors influencing the prevalence of ghost worker fraud, such as weaknesses in payroll management, governance gaps, and perceived inefficiencies of IPPIS.

A Five-Point Likert Scale (Strongly Disagree = 1; Somewhat Disagree = 2; Neutral = 3; Somewhat Agree = 4; Strongly Agree = 5) was adopted to measure the strength of respondents' perceptions. This scale allowed for systematic quantification of attitudes toward IPPIS effectiveness, transparency, and fraud prevention.

Although the survey questions were designed to align with the study's objectives, focusing on IPPIS performance, transparency, and fraud elimination, an explicit mapping table was not included for this phase. The direct nature of the questions ensured clarity in addressing the research objective one without requiring additional mapping.

### 4.2.1 Ethical consideration

During the study process, ethical concerns were carefully followed. The Department of Computer and Information Sciences approved the ethics application of 2021 surveys with the application ID of 1527 (see Appendix B). This ensures that the study followed the rules for ethical research involving participants. Participants in the surveys gave their informed consent after being informed about the nature of the study. Participants were told that their responses would be kept anonymous and used only for the purpose of this research. The ethical integrity of the research process was maintained to ensure that the results are credible, respectful and conducted in accordance with established research ethics.

### 4.2.2 Pilot Testing and Instrument Evaluation

Pilot studies are small-scale versions of full-scale studies designed to test logistics, gather information, and improve overall research design before larger implementation [409]. It helps identify design flaws, assess feasibility, and improve the reliability and

validity of instruments before full-scale deployment. Research Validity is defined as the extent to which the data-gathering tool evaluates what it intends to measure, it focuses on the accuracy of the data-gathering instrument [355]. Validity is of different types and suggest that construct validity is generally accepted in research and is based on relationships [383]. On the other hand, reliability focuses on data collection tool that consistently returns similar results on the same participants, this will prevent the researcher from properly formulating or generalizing theories to an increasing number of users [110].

**Methodological approach of pilot testing**

Participants were federal government employees enrolled on the IPPIS platform. The questionnaire was administered through the WhatsApp platform. The pilot instrument included items grouped into thematic categories aligned with the study's conceptual framework, including perceived effectiveness of IPPIS, trust in system integrity, likelihood of fraud reduction etc. Respondents were asked to rate each item using a 5-point Likert scale. In this study, the pilot test was conducted to evaluate the clarity, consistency, and reliability of a 14-item questionnaire designed to assess perceptions of IPPIS effectiveness and its link to ghost worker fraud in the Nigeria public sector.

**Reliability Analysis**

This study used Cronbach's alpha reliability coefficient "$\alpha > 0.7$" to measure the survey questionnaire for internal reliability using SPSS. The idea is to determine internal consistency of scale, and how consistent people respond to the questions. The results are presented in Table 4.1. The pilot result in Table 4.1 shows that Cronbach's alpha efficiency of 0.740, which is an acceptable value because it is higher than the reference value of 0.7 [163]. The result suggests that the items are reasonably correlated and measure a coherent construct.

Table 4.1: Reliability Statistics for Pilot Test

| **Statistic** | **Value** |
|---|---|
| Cronbach's Alpha | 0.740 |
| Number of Items | 14 |

## 4.3 Confidence Interval Analysis

Confidence intervals (CIs) serve as a fundamental tool for estimating the range within which the true population parameter is likely to fall, based on sample data. In the context of the 2021 survey, CIs was calculated for 9 items to determine whether the sample responses reliably reflect the broader population of public sector employees in Nigeria. This approach is particularly important given the study's aim to evaluate perceptions of employment integrity of the existing employment system. By establishing confidence intervals around the sample means, we assess not only the central tendency of responses but also the precision and generalizability of these findings.

### 4.3.1 Methodology

The confidence interval for a mean is typically calculated as:

$$\text{CI} = \bar{x} \pm z \left( \frac{\sigma}{\sqrt{n}} \right)$$

Where:

- $\bar{x}$ is the sample mean
- $z$ is the z-score corresponding to the desired confidence level (e.g., 1.96 for 95%)
- $\sigma$ is the sample standard deviation
- $n$ is the sample size

In this study, the CI bounds were derived from descriptive statistics, and the Error ($\pm$) was computed as: Error ($\pm$) = UpperCI - Mean This error margin reflects the extent to which the sample mean might deviate from the true population mean. Narrow

intervals suggest high precision and confidence in the representativeness of the sample, while wider intervals indicate greater uncertainty.

### 4.3.2 2021 Survey Confidence Interval Data Presentation and Analysis

Below is the presentation and analysis of the CIs of 2021 survey, including the data table.

Table 4.2: Confidence Interval Summary for 2021 Survey Questions

| **Question** | **Mean** | **LowerCI** | **UpperCI** | **Error (±)** |
|---|---|---|---|---|
| IPPIS gives equal opportunity to qualified applicants during recruitment | 1.88 | 1.66 | 2.10 | 0.22 |
| Removal of ghost workers from IPPIS give others chance to be employed | 3.69 | 3.41 | 3.97 | 0.28 |
| There is no room for Ghost Workers in IPPIS | 2.32 | 2.02 | 2.62 | 0.30 |
| The IPPIS payroll system has promoted accountability in the payroll administration compared to the previous GIFMIS | 2.50 | 2.20 | 2.80 | 0.30 |
| Data in the IPPIS is highly protected | 2.65 | 2.37 | 2.93 | 0.28 |
| Superior staff of IPPIS have no hand in ghost worker fraud | 2.82 | 2.54 | 3.10 | 0.28 |
| IPPIS is always open for data audit | 2.82 | 2.54 | 3.10 | 0.28 |
| It is easier to trace fraud now than with the previous system (GIFMIS) | 2.66 | 2.38 | 2.94 | 0.28 |
| There are cases of cyberattacks on the IPPIS | 3.43 | 3.19 | 3.67 | 0.24 |

#### Conclusion

The confidence interval analysis in summary Table 4.2 highlight the degree of certainty in how well the sample reflects broader public opinion. For instance, the item "There are cases of cyberattacks on the IPPIS" had a high mean (3.43) and a narrow margin of

error (±0.24), indicating strong agreement among respondents and suggesting that the sample likely represents the wider population's views on this issue. The low variability enhances confidence in generalizing this finding. In contrast, the item "There is no room for Ghost Workers in IPPIS" had a lower mean (2.32) and a wider error margin (±0.30), pointing to more diverse or uncertain opinions. This wider interval reflects greater variability in responses and reduces confidence in the sample's representativeness for this item. Overall, these insights help assess the perceived integrity of IPPIS in 2021 and guide comparisons with future surveys.

## 4.4 Data presentation and analysis

The data collected were quantitative and were collected using the online Qualtrics survey tool [121]. There were 145 responses to the questionnaire from personnel of the Nigerian Federal Civil Service. Descriptive statistics was used to interpret employees' responses. Below are the tables and bar charts for 1 to 9 questions with their corresponding explanations. Based on information on Table 4.3 and Figure 4.1, a decisive

Table 4.3: IPPIS gives equal opportunity to qualified applicants during recruitment

| Response | Count | Percentage |
|---|---|---|
| Strongly Disagree | 94 | 65.3% |
| Somewhat Disagree | 18 | 12.5% |
| Not Applicable | 3 | 2.1% |
| Somewhat Agree | 14 | 9.7% |
| Strongly Agree | 15 | 10.4% |
| Total | 144 | 100.0% |

77.8% of employees disagreed that IPPIS provides equal opportunity in recruitment, with only 20.1% expressing agreement. This reflects a widespread perception that recruitment into the system remains non-transparent and subject to manipulation. Such scepticism suggests that IPPIS, while digitised, has not removed discretionary control over recruitment, leaving room for nepotism and corruption. A strong majority (65.9%) agreed that removing ghost workers creates opportunities for genuine employment as shown in Table 4.4 and Figure 4.2. This indicates an awareness among

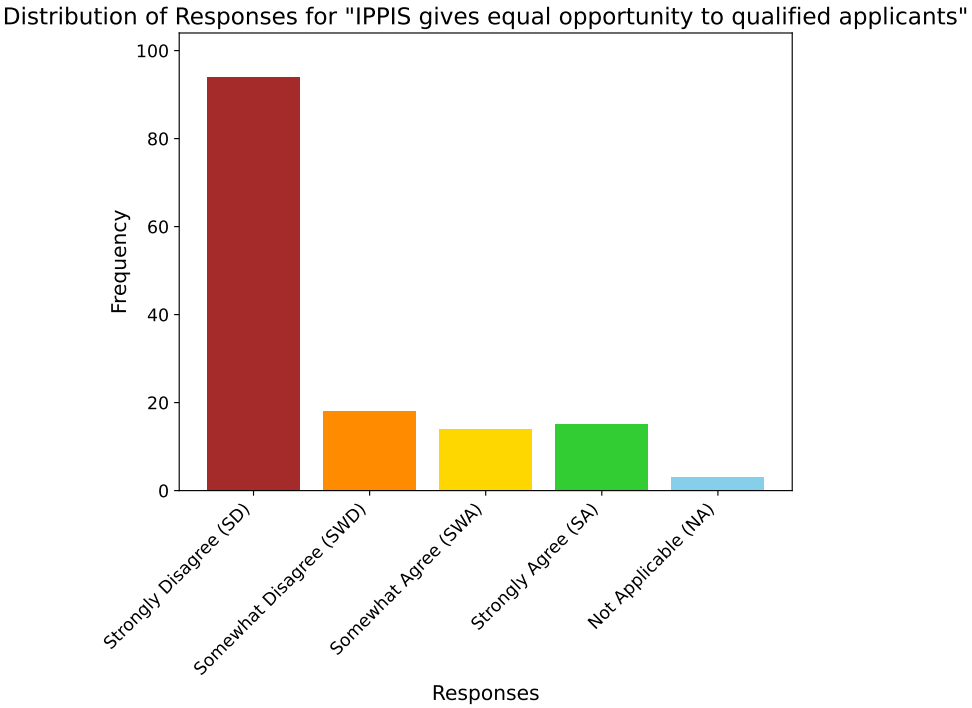


Figure 4.1: IPPIS gives equal opportunity to qualified applicants during recruitment

Table 4.4: Removal of ghost workers give others chance to be employed

| Response | Count | Percentage |
|---|---|---|
| Strongly Disagree | 25 | 17.7% |
| Somewhat Disagree | 13 | 9.2% |
| Not Applicable | 10 | 7.1% |
| Somewhat Agree | 26 | 18.4% |
| Strongly Agree | 67 | 47.5% |
| Total | 141 | 100.0% |

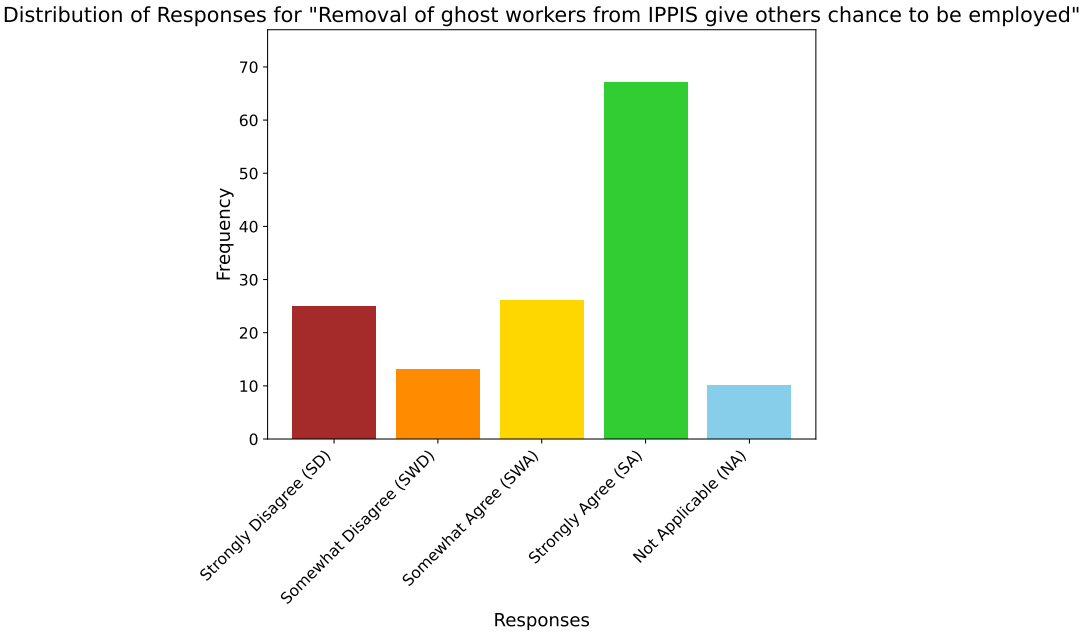


Figure 4.2: Removal of ghost workers from IPPIS gives others a chance to be employed

employees that fraudulent payroll practices not only drain resources but also crowd out legitimate candidates. It reinforces the perception that payroll integrity is directly linked to job creation and employment process in the public sector. From Table 4.5

Table 4.5: There is no room for Ghost Workers in IPPIS

| Response | Count | Percentage |
|---|---|---|
| Strongly Disagree | 75 | 53.6% |
| Somewhat Disagree | 18 | 12.9% |
| Not Applicable | 3 | 2.1% |
| Somewhat Agree | 15 | 10.7% |
| Strongly Agree | 29 | 20.7% |
| Total | 140 | 100.0% |

and Figure 4.3, two-thirds of employees (66.4%) rejected the idea that IPPIS fully eliminates ghost workers, underscoring deep scepticism about the system's effectiveness. This aligns with ongoing public discourse about continued payroll fraud despite IPPIS adoption. According to the findings in Table 4.6 and Figure 4.4, a majority (60.7%) disagreed that IPPIS improved accountability compared to GIFMIS, while

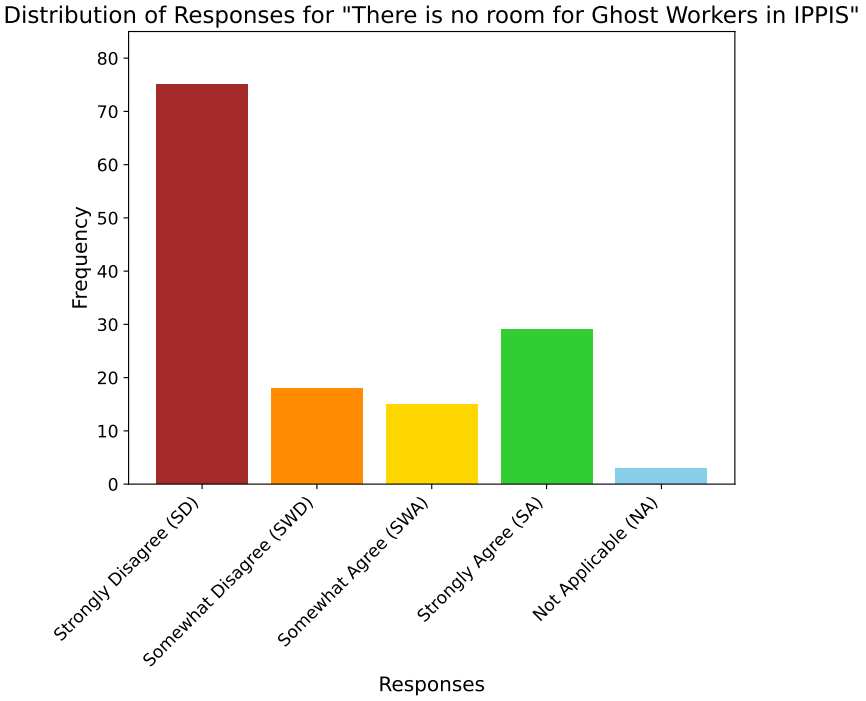


Figure 4.3: There is no room for Ghost Workers in IPPIS

Table 4.6: The IPPIS payroll system has promoted accountability in the payroll administration compared to the previous GIFMISS

| Response | Count | Percentage |
|---|---|---|
| Strongly Disagree | 57 | 43.8% |
| Somewhat Disagree | 22 | 16.9% |
| Not Applicable | 5 | 3.8% |
| Somewhat Agree | 21 | 16.2% |
| Strongly Agree | 25 | 19.2% |
| Total | 130 | 100.0% |

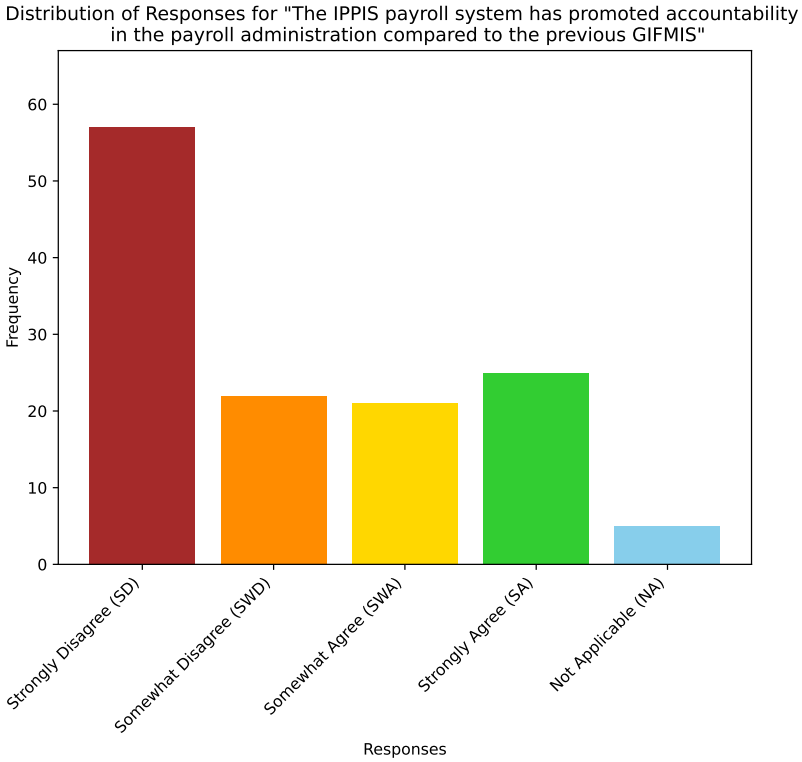


Figure 4.4: The IPPIS payroll system has promoted accountability in the payroll administration compared to the previous GIFMIS

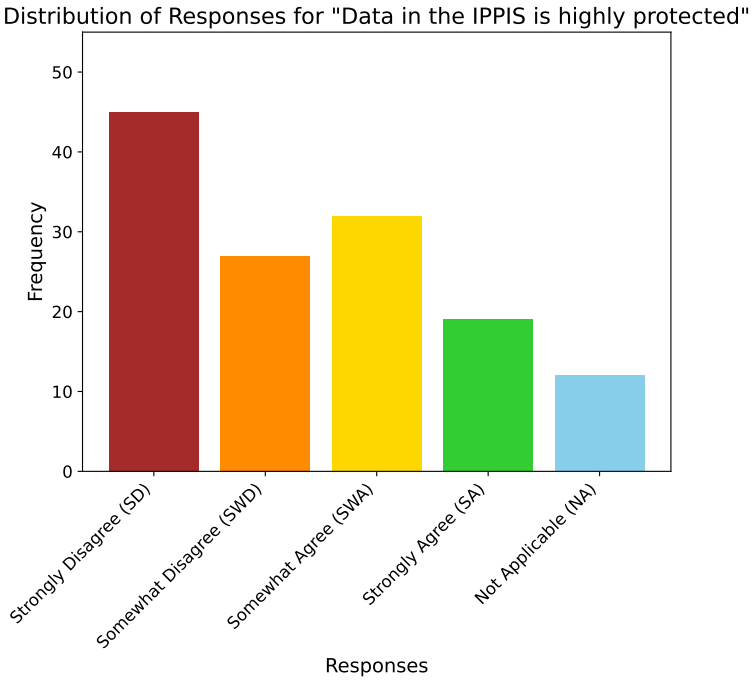


Figure 4.5: Data in the IPPIS is highly protected

35.4% agreed. This reveals a trust deficit in IPPIS's promise of better transparency, suggesting that digitisation has not overcome entrenched perceptions of payroll and employment mismanagement. Looking at Table 4.7 and Figure 4.5, over half of

Table 4.7: Data in the IPPIS is highly protected

| Response | Count | Percentage |
|---|---|---|
| Strongly Disagree | 45 | 33.3% |
| Somewhat Disagree | 27 | 20.0% |
| Not Applicable | 12 | 8.9% |
| Somewhat Agree | 32 | 23.7% |
| Strongly Agree | 19 | 14.1% |
| Total | 135 | 100.0% |

employees (53.3%) doubted that IPPIS data was well-protected, while only 37.8% expressed confidence. This highlights significant employee concerns about the security of sensitive payroll data, with implications for trust in digital governance systems. From Table 4.8 and Figure 4.6, Two-thirds (66.9%) of respondents suspected superior

Table 4.8: Superior staff of IPPIS have no hand in ghost worker fraud

| Response | Count | Percentage |
|---|---|---|
| Strongly Disagree | 54 | 41.5% |
| Somewhat Disagree | 33 | 25.4% |
| Not Applicable | 19 | 14.6% |
| Somewhat Agree | 17 | 13.1% |
| Strongly Agree | 7 | 5.4% |
| Total | 130 | 100.0% |

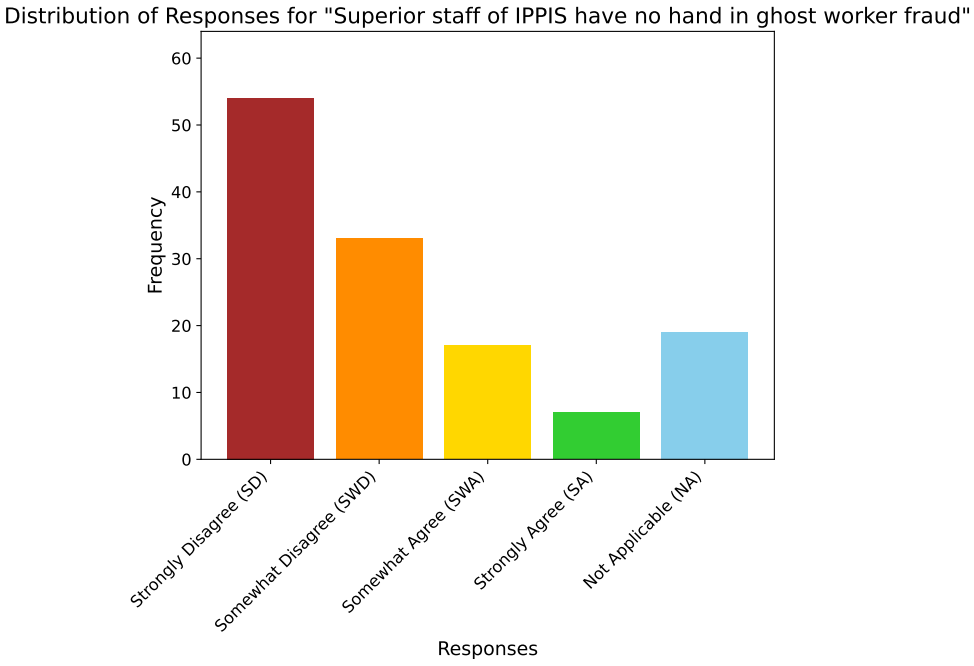


Figure 4.6: Superior staff of IPPIS have no hand in ghost worker fraud

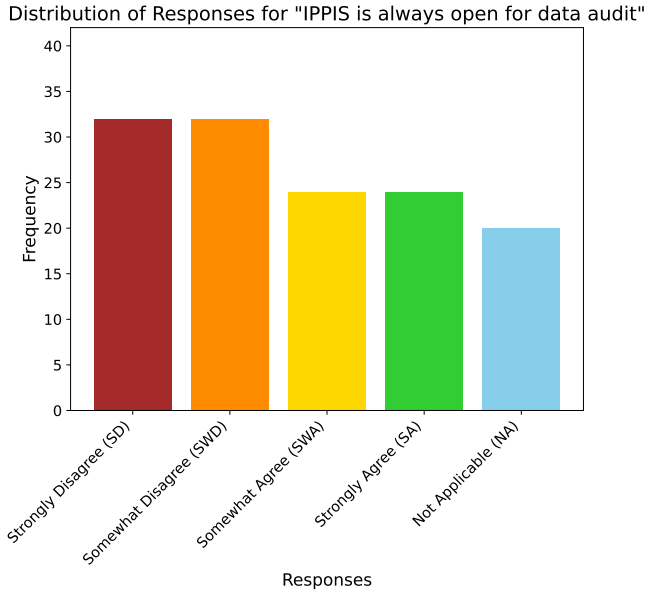


Figure 4.7: IPPIS is always open for data audit

staff of involvement in ghost worker fraud. This deep mistrust of senior management suggests that fraud is perceived as systemic, not merely incidental. It aligns with wider literature implicating senior officials in payroll manipulation. Nearly half (48.5%)

Table 4.9: IPPIS is always ready for data audit

| Response | Count | Percentage |
|---|---|---|
| Strongly Disagree | 32 | 24.2% |
| Somewhat Disagree | 32 | 24.2% |
| Not Applicable | 20 | 15.2% |
| Somewhat Agree | 24 | 18.2% |
| Strongly Agree | 24 | 18.2% |
| Total | 132 | 100.0% |

in Table 4.9 and Figure 4.7 doubted IPPIS's readiness for audit, while only 36.4% were confident. A further 15.2% selected "Not Applicable," suggesting limited access to audit processes. This reflects inconsistent perceptions of accountability and transparency. Considering Table 4.10 and Figure 4.8, a majority (53.3%) believed fraud was not easier to trace under IPPIS, compared to 39.1% who believed it was. This division highlights persistent doubts about the system's fraud detection capabilities. Almost

Table 4.10: It is easier to trace fraud now than with the previous system (GIFMIS)

| Response | Count | Percentage |
|---|---|---|
| Strongly Disagree | 53 | 39.8% |
| Somewhat Disagree | 18 | 13.5% |
| Not Applicable | 10 | 7.5% |
| Somewhat Agree | 25 | 18.8% |
| Strongly Agree | 27 | 20.3% |
| Total | 133 | 100.0% |

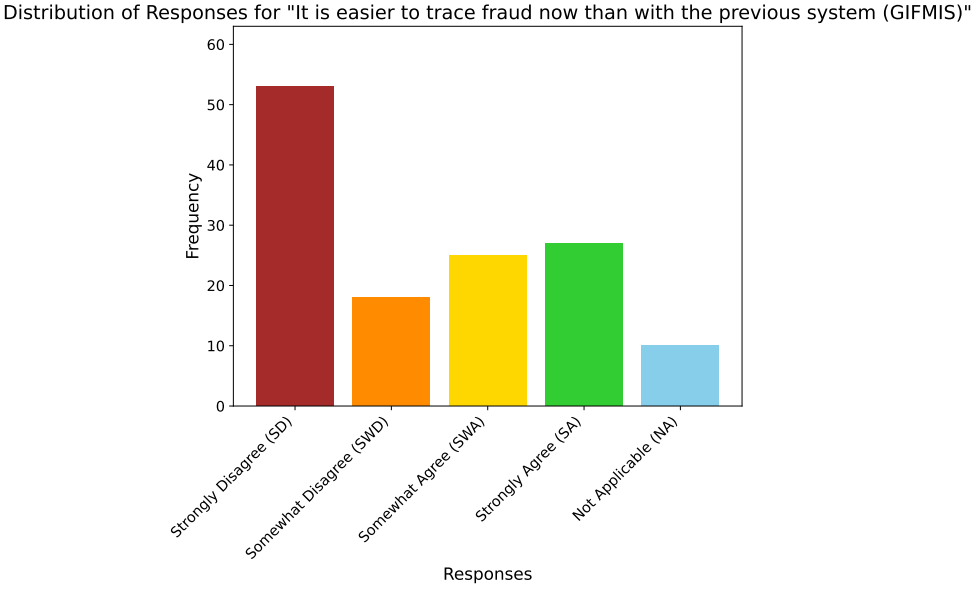


Figure 4.8: It is easier to trace fraud now than with the previous system (GIFMIS)

Table 4.11: There are cases of cyberattacks on the IPPIS

| Response | Count | Percentage |
|---|---|---|
| Strongly Disagree | 15 | 10.9% |
| Somewhat Disagree | 13 | 9.5% |
| Not Applicable | 41 | 29.9% |
| Somewhat Agree | 34 | 24.8% |
| Strongly Agree | 34 | 24.8% |
| Total | 137 | 100.0% |

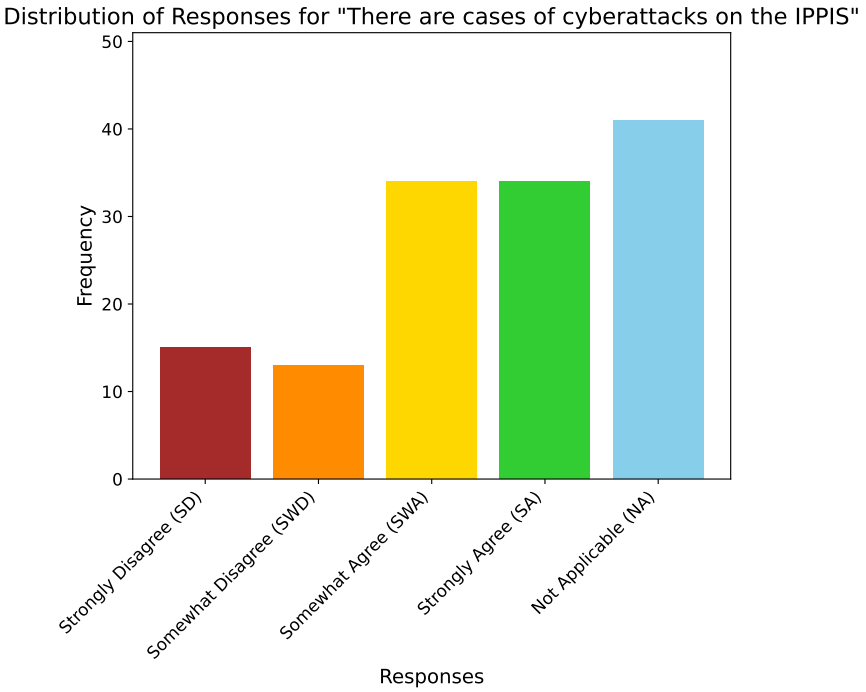


Figure 4.9: There are cases of cyberattacks on the IPPIS

half of respondents (49.6%) agreed that cyberattacks occur on IPPIS as shown in Table 4.11 and Figure 4.9, while 20.4% disagreed and 29.9% reported "Not Applicable." This mixed response suggests uneven awareness of cybersecurity issues. The significant proportion citing attacks reflects broader concerns about the system's vulnerability, a recurring theme in Nigeria's digital governance initiatives.

## 4.5 Conclusion

The findings from the 2021 survey reinforce the literature reviewed in Chapter 2, which highlighted persistent transparency and integrity challenges within the IPPIS system. Responses reveal a significant trust deficit among federal government employees, with widespread skepticism regarding IPPIS's ability to ensure transparency, eliminate ghost workers, and maintain robust data security. While some participants acknowledged marginal improvements compared to previous payroll systems, the overall perception suggests that IPPIS has not completely solved the issue of ghost worker fraud and con-

tinues to exhibit systemic vulnerabilities such as insider manipulation and weak audit readiness. These insights underscore the need for structural reforms and stronger mechanisms to enhance accountability and restore confidence in public sector employment processes.

# Chapter 5

# Ethereum Besu Concept

Blockchain technology was selected as the foundational solution for this research because of its inherent ability to address the core challenges identified in Chapter 2—namely, transparency, integrity, and fraud prevention in public sector employment process. Traditional centralized systems such as IPPIS concentrate control within a single authority, creating vulnerabilities that enable ghost worker fraud and insider manipulation. Blockchain, by contrast, introduces decentralization, distributing validation and decision-making across multiple nodes, thereby reducing single points of failure and enhancing trust in the employment process. The proposed design leverages the Ethereum Besu platform, a permissioned blockchain framework suitable for enterprise and government use cases. This choice aligns with the study's objectives by enabling secure, auditable, and transparent transactions through smart contracts. Smart contracts automate critical steps in employee verification, ensuring that predefined rules govern every transaction without manual interference. This automation strengthens accountability and minimizes human error, while the decentralized architecture ensures that no single entity can manipulate records undetected. By integrating these features, the design operationalizes theoretical principles of transparent governance into a practical, technology-driven solution for mitigating ghost worker fraud.

Therefore, it is necessary to discuss the Ethereum Besu concept to give a complete picture as a means to address the issue of ghost worker fraud. The concept comprises of a brief overview of decentralization, smart contracts, and the Ethereum Besu platform. Blockchain technology revolutionises governance systems by providing decentralized frameworks that distribute authority and decision-making among a network of nodes. Decentralization is not only an abstract idea, but a basic principle that supports the integrity of the offered solution. Decentralizing the recruitment process in the Nigerian

public sector helps to reduce the danger of fraud and corruption that is inherent in centralized systems such as the IPPIS. This decentralization is in accordance with the theoretical arguments presented by authors such as Arkorful et al. and Faguet who highlight the significance of trust, transparency, and accountability in governance [34] [133]. Using blockchain technology, the goal is to implement these ideas and transform theoretical principles into effective solutions for preventing ghost worker fraud.

Moreover, the incorporation of smart contracts and the Ethereum Besu platform introduces an additional level of automation and transparency to the employment procedure. Smart contracts, which are regulated by predetermined criteria, simplify the process of verifying and approving new personnel, hence minimizing the chances of human mistakes and manipulation. This automation not only improves efficiency but also strengthens the theoretical basis of transparent governance. Stakeholders participating in the Private Ethereum Besu blockchain platform engage in a process that is both visible and auditable, thanks to the use of smart contracts. Therefore, the framework presented in this chapter acts as the foundation for creating and executing a strong solution that utilizes blockchain technology to successfully address ghost worker fraud.

## 5.1 Decentralization and transparency in governance

Blockchain platforms provide opportunity to investigate different governance structures and construct a theory of the utility of centralized, semi-decentralized, and decentralized governance. Decentralization here refers to the degree to which the political, administrative, or fiscal authority of a central government has been delegated to subnational agencies or authorities that are geographically and organizationally dispersed [99]. This governmental decentralization in practice encompasses a range of forms, each founded on distinct principles and for various aims. Arkorful et al. [34] investigated the relationship between decentralization and public engagement, using trust and transparency as mediators. The outcome demonstrates the importance of trust and transparency in decentralization and participation.

According to Faguet [133], the most fundamental theoretical reason for decentral-

ization is that it can increase government accountability and responsiveness to the governed. Thus, decentralized governance ideas apply to many industries beyond blockchain technology, for example, the renewable energy industry has witnessed the implementation of decentralized governance through the implementation of community-based energy initiative projects [162]. Solar panels and wind turbines are examples of renewable energy sources that are managed and operated by local communities through joint efforts in these programs. Besides blockchain, decentralized governance models have changed political, administrative, and organizational systems [449]. Political scientists, sociologists, and public administrators have studied how decentralization affects government, citizen involvement, and public service delivery. By using these interdisciplinary perspectives, we can better comprehend decentralized governance and its consequences for complex social issues beyond ghost worker fraud.

Additionally, decentralized governance models are used in urban planning, environmental management, and community development [140]. Subsidiarity, participatory decision-making, and polycentric governance emphasize local stakeholder responsibility and collaborative governance networks. This research places blockchain-based decentralized governance in a theoretical and practical context by drawing from these fields.

However, Y. Chen et al. compared centralization with decentralization and found semi-decentralization to be better for governance [90]. Some other literature [90] [91] [281] suggests that decentralization reverses the traditional relationship between platform market capitalization, developer interest, and development activity—shifting the primary driver from market size to community-driven development and innovation. Further analysis in the context of blockchain architecture, the platform for governance decentralization determinants shows that infrastructure-layer digital platforms tend to become more decentralized than application-layer ones. Y. Chen et al.' research sheds light on platform governance's causes, effects, and characteristics [90].

Blockchain technology emphasizes decentralization, which distributes authority and decision-making over a network of nodes. Decentralization can improve governance transparency, accountability, and censorship and manipulation resistance. Decentral-

izing the Nigerian public sector employment process might reduce fraud and corruption risk compared with centralized systems like the IPPIS. Governance also requires transparency, taking actions, decisions, and procedures transparent to stakeholders. Stakeholders could verify data integrity and authenticity without intermediaries using blockchain technology's tamper-evident and immutable transaction record.

## 5.2 Solidity, smart contracts and automation of processes

The Ethereum platform uses Solidity programming language for smart contracts development [257]. The language is built upon the Ethereum virtual machine. Solidity's primary function is to store every state of the tokens that the nodes send and receive. Programmers with prior familiarity in Python, C++, or JavaScript should have little trouble understanding Solidity [258]. Smart contracts are contracts that self-execute based on established criteria and parameters. Smart contracts are critical in this framework because they enable automation of the validation and approval process for new employees. Smart Contracts can be programmed to execute a certain transaction only if it receives approval from a specified number of nodes in the network, conforming consensus and security. In the context of this study, smart contracts play an essential part in the automation of the employment process. This includes the validation and approval of new employees by a number of different government bodies.

### 5.2.1 Ethereum Besu

Ethereum Besu is a blockchain platform designed for enterprises, enabling them to use blockchain technology for identity verification, financial services, supply chain management and some governmental functions [350]. It is an open-source blockchain architecture as shown in Figure 5.1 that is part of the Ethereum ecosystem and offers flexible permissioning capabilities, enhanced privacy features, and robust performance. Its compatibility with the Ethereum Virtual Machine (EVM) ensures smooth operation with existing Ethereum-based applications and smart contracts [398]. Ethereum Besu also provides advanced-level deployments with support for consensus algorithms like

Proof of Authority, Proof of Work, and Istanbul Byzantine Fault Tolerance.

The proposed framework adopts a permissioned consensus model optimized for performance within a consortium of legally accountable public-sector validators. The threat model assumes regulated institutional actors operating under statutory and audit constraints rather than arbitrary Byzantine adversaries. Although Byzantine fault-tolerant consensus offers stronger adversarial guarantees [87], it introduces additional latency and operational complexity that may be disproportionate in controlled governmental environments.

Importantly, the framework redistributes rather than eliminates trust. Unlike traditional PKI-based systems, which centralize authority within a single administrative domain, blockchain-based architectures enable distributed validation, replicated state, and tamper-evident auditability across multiple entities [445]. This reduces single-point manipulation risk while maintaining institutional accountability. Although public trust in government entities may vary, the framework introduces structural safeguards through multi-agency validation and immutable record-keeping rather than relying on unilateral administrative control.

Ethereum Besu is an Ethereum client that has been developed by ConsenSys and is open-source. It has been specifically built to cater to enterprise use cases that necessitate exceptional performance, scalability, and anonymity. Besu, functioning as a permissioned Ethereum client, provides a range of features and capabilities specifically designed to cater to the requirements of organizations operating inside regulated milieus. The following below are the key features and capabilities:

### Permissioning models

Ethereum Besu offers a number of different permissioning models, which let organizations set up access controls and governance policies that are perfect for their needs. With these permissioning models, businesses and organizations can limit who can access the blockchain network, manage the roles and permissions of participants, and apply governance rules to keep the network safe and in line with regulations. In this work, there are eight participants in the Besu network with different permissions and

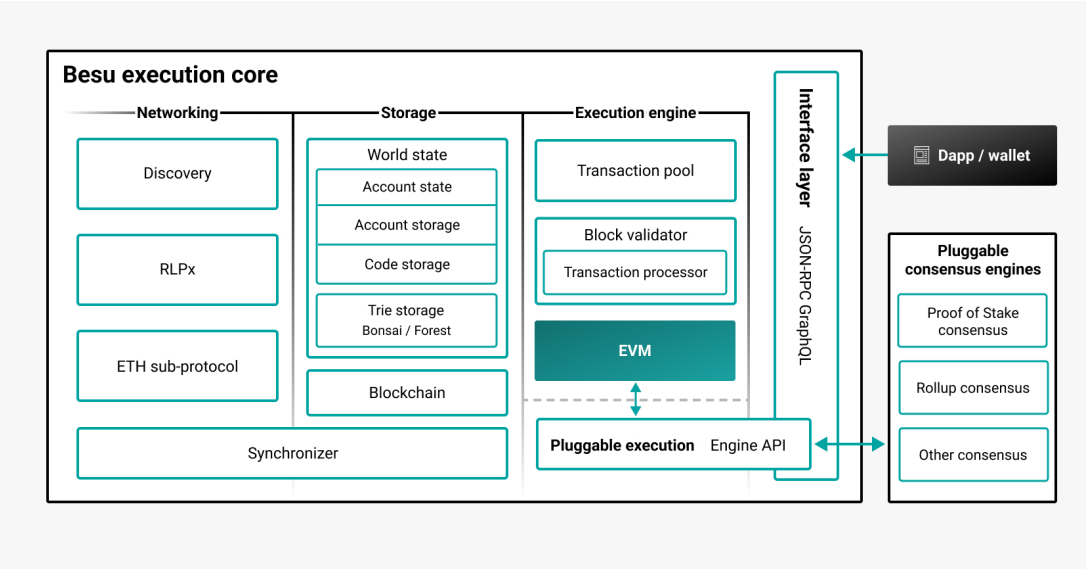


Figure 5.1: Ethereum Besu Architecture[59]

responsibilities.

### Consensus algorithms

Ethereum Besu supports a number of different consensus algorithms, such as Proof of Authority (PoA), Proof of Work (PoW), and Istanbul Byzantine Fault Tolerance (IBFT). In this study, Proof of Authority which is a variant of the Practical Byzantine Fault Tolerant algorithm was adopted. Practical Byzantine Fault Tolerant algorithm is suitable for blockchain applications with limited number of trusted nodes [433] and the algorithm as non-proof-of-work avoids the high energy consumption and other mining complexities.

### Proof of authority (PoA)

Proof of Authority is a mechanism that is intended to improve the Proof of Stake mechanism and is preferably utilized in permissioned networks. PoA picks a small group of nodes as transaction validators based on their identity or reputation staked in the network [146]. This is in contrast to the traditional method of selecting block miners, which is based on the amount of cryptocurrency tokens they have staked in. The Proof

of Authority (PoA) consensus mechanism in Besu is necessary for the implementation of private transactions, and it would provide immediate finality [315]. Validators in the Besu network are the user accounts that have been permitted to validate private transactions and blocks. In the context of this work, four agencies represent the validators; FCC, IPPIS, CBN, and the Ministry concerned. All these agencies are the authorities that are selected to stand as the validators. They must all approve a certain transaction before the transaction would be appended on the blockchain and become legal.

#### Better privacy

To keep private information safe in the blockchain network, Ethereum Besu includes advanced privacy features such as private transfers and confidential contracts [261]. Companies can now use these privacy improvements to make transactions safer and more private while still protecting data privacy and security. This is especially important for apps that deal with personal information and financial transactions.

#### Performance optimization

According to Capital, Ethereum Besu is built for enterprise-level performance, and it has been optimized to speed up transactions and lower delay [84]. These improvements to performance make sure that the blockchain network can handle a considerable number of transactions without any problems. This allows enterprise apps to grow without sacrificing security or decentralization.

#### Corporate support and maintenance

Because Ethereum Besu is part of the ConsenSys ecosystem, it receives strong corporate support and maintenance services, such as technical support, training, and documentation. This makes sure that companies using Ethereum Besu can get the tools and help they need to create, use, and manage blockchain solutions correctly.

These assertions are supported by the fact that JPMorgan Chase has been able to achieve success using Quorum, which is a version of Ethereum that is geared towards business applications. The Quorum offers enhanced privacy, security, and performance

features suitable for enterprise use [316]. It supports confidentiality in smart contracts and transactions, as well as crash and Byzantine fault-tolerant consensus algorithms [42]. Quorum's potential has been explored in various sectors, including parking management systems for business entities, focusing on privacy, performance, and scalability [186]. Additionally, Quorum has been utilized to create auditable frameworks for data aggregators in permissioned blockchain settings, enabling secure and transparent data market mechanisms [366]. These applications showcase Quorum's versatility and effectiveness in addressing enterprise blockchain needs, supporting its success in business-oriented implementations of blockchain technology.

This demonstrates the level of confidence that large financial organizations have in ConsenSys' capabilities. Quorum was initially built by JPMorgan Chase, then in the year 2020 [364], it was transferred to ConsenSys. As a result of this transfer, Quorum has been able to take advantage of the enormous experience, support, and development resources that ConsenSys possesses, which has resulted in an increase in its acceptance and functionality across the financial sector. Ethereum Besu's corporate backing is strengthened in terms of its dependability and credibility as a result of the success of Quorum and the smooth transition of its administration to ConsenSys. This demonstrates the company's capacity to provide high-quality support and maintenance for blockchain solutions.

## 5.3 Operational Architecture of Ethereum Besu

Ethereum's protocol implements a replicated state machine, with the Ethereum Virtual Machine (EVM) executing smart contracts written in bytecode [86]. The EVM is a key component of Ethereum, providing a deterministic but practically unbounded state machine with globally accessible state and virtual machine capabilities [103]. KEVM, a formal semantics of the EVM, has been developed to enhance security and enable rigorous program analysis [172]. While Ethereum traditionally uses Ethash for consensus on the mainnet, private blockchain implementations like Besu and Quorum, both built on the EVM, offer alternatives for enterprise use. It is often deployed with

permissioned consensus algorithms such as Clique (PoA) and IBFT 2.0 (IBFT) which ensures immediate finality and robustness in eventually synchronous networks [349].

In a permissioned blockchain setting like DEIFP, Ethereum Besu provides the following functionalities:

1. Consensus Configuration: Besu can be configured with either Clique or IBFT 2.0 through the genesis file, determining how blocks are proposed and validated, just as an illustration shown below.

2. Node Permissioning: Access to participate in block validation can be restricted using smart contract-based or file-based permissioning.

3. Privacy via Tessera: Supports private transactions between specified nodes using Tessera, ensuring confidentiality.

4. Monitoring and Telemetry: Enterprise APIs enable integration with dashboards and monitoring tools for performance evaluation.

   Besu's modular architecture enables developers to design secure and permissioned blockchain networks aligned with institutional structures.

```
{
  "config": {
    "chainId": 1337,  // Unique chain ID
    "muirglacierblock": 0,
    "berlinblock": 0,
    "byzantiumblock": 0,
    "constantinopleblock": 0,
    "clique": {
      "period": 15,  // Block time in seconds
      "epoch": 30000
    }
  },
  "nonce": "0x0",
  "timestamp": "0x58ee40ba",
  "extraData": "0x00000000000000f842...544c5b2",
  "gasLimit": "0x47b760",
```

```
17      "difficulty": "0x1",
18      "mixHash": "0x6374696368616 96e0...00000",
19      "coinbase": "0x000000000000000...00000",
20      "alloc": {
21        "0x0a57fcb9911072177f598b0c326492dd52031193": { "balance":
    "10000000000000000000000" },
22        "0xf1ed5a9ad48e2794de45674f3e6dc9e21d5fbe76": { "balance":
    "10000000000000000000000" }
23      }
24    }
25
```

Listing 5.1: Genesis Configuration File

## 5.4 Security Properties of Ethereum Besu

Ethereum Besu inherits critical security guarantees from Ethereum's design principles while offering additional assurances through permissioned consensus. These properties are essential for ensuring the reliability and trustworthiness of the proposed framework.

Besu, when configured with PoA or IBFT, aligns with security assumptions [134] [2], which formalizes blockchain safety and liveness under partial synchrony. Although DEIFP does not use Nakamoto consensus, similar assumptions about validator honesty and communication delays underlie IBFT.

## 5.5 Justification of Clique (Proof of Authority) for DEIFP

In the proposed DEIFP's framework, Clique is chosen due to its lightweight configuration and suitability for networks with a limited number of known validators. Blocks are signed by a rotating leader selected from the validator list. Clique's block interval and block period settings allow it to achieve rapid finality.

According to Islam et al., PoA Clique offers low computational requirements, sufficient for semi-trusted institutional networks and better suited for networks with regulatory oversight and well-defined membership [189].

| **Security Property** | **How Ethereum Besu Ensures It** | **Related Literature / Protocols** |
|---|---|---|
| Safety | Blocks are validated by a majority of authorized validators. Clique uses a stable fork choice rule and delays to ensure consistency. IBFT 2.0 provides finality by waiting for 2/3+ consensus before appending blocks. | [349]; [58]; [222]; [145]; Ethereum Yellow Paper; IBFT 2.0 Protocol |
| Liveness | Network continues to produce blocks as long as less than 1/3 of validators are faulty (IBFT 2.0). In Clique, new blocks are signed at fixed intervals to guarantee progress. | [349]; [260]; [145]; [182] |
| Immutability | Every block includes a hash of the previous block, creating a tamper-evident, append-only ledger. | [274]; [322] |
| Non-repudiation | Transactions are signed using ECDSA, ensuring provenance and accountability. | [218]; [403]; [324] |
| Availability | Network replication across validators and observer nodes ensures redundancy and service continuity. | [280]; [131] |
| Confidentiality | Tessera handles private payloads using encrypted messaging and designated recipient groups. | [134] |

Table 5.1: Summary of Security Properties in Ethereum Besu and Relevant Literature

Validators in DEIFP include:

- IPPIS: Responsible for payroll processing and employment records.
- FCC: Ensures compliance with public sector ethics and standards.
- CBN: Oversees salary disbursement and fiscal governance.
- Relevant Ministries: Own and validate sector-specific employment entries.

These are considered trusted nodes because they operate independently, possess regulatory mandates, and are accountable to different government oversight structures.

However, conditional trust is acknowledged—while trusted to validate data, their actions are still logged and observable by non-validating observer nodes such as the EFCC, Police and Judiciary, providing external deterrence.

## 5.6 Alternatives for Scalable Decentralization

As DEIFP grows from a small consortium of trusted government agencies to potentially include hundreds of ministries, state agencies, NGOs, and external validators, relying solely on Clique (Proof of Authority) would introduce significant risks. Clique assumes a semi-trusted environment and does not handle Byzantine faults (e.g., malicious validators) [129]. Therefore, scalable and robust consensus mechanisms become critical. Below, we explore alternatives in depth:

**IBFT 2.0 Consensus Type:** Byzantine Fault Tolerant algorithm designed to handle malicious actors [235]. It possess strong finality, once a block is confirmed by two thirds of validators, it cannot be reversed [376]. In addition, its fault tolerance of maintaining network integrity and liveness as long as fewer than 1/3 of validators act maliciously or fail [225]; [118]. In terms of communication, validators exchange multiple rounds of signed messages to reach consensus, ensuring no forks. BFTree allows Byzantine Fault Tolerance consensus to scale to millions of validators without forks by arranging them in a virtual tree to parallelize signature aggregation [29]. And finally, applicability, well-suited for larger permissioned networks where validators are known but potentially geographically dispersed or representing different organizations [160].

Benefit to DEIFP: Enables inclusion of more validators without sacrificing security, while still allowing observers to monitor the network.

**Proof of Stake Variants Consensus Type:** Recent research explores economic security-based consensus mechanisms in proof-of-stake (PoS) systems where validators stake tokens [116]. Finality is achieved through penalties and rewards; validators who act maliciously lose their stake. Finality ensures consistency even in partially-

synchronous environments, while accountable safety allows for identifying malicious validators [279]. These properties are achieved through a combination of rewards and penalties [159]. PoS is suitable for public or hybrid networks where validators might be anonymous or semi-anonymous. It is currently not supported natively in Besu for private networks. Introducing staking mechanisms would require a significant economic and technical redesign, which can conflict with the institutional focus of DEIFP.

Future Potential: As DEIFP evolves into a semi-public network, Proof of Stake could help democratize validation and reduce reliance on institutional trust.

**HotStuff BFT Consensus Type:** HotStuff is a leader-based Byzantine fault-tolerant replication protocol optimized for scalability with linear communication complexity and responsiveness [438] adopted by Meta's Diem (formerly Libra) and other large-scale projects [317]. Achieves linear communication complexity, reducing bottlenecks when hundreds of validators participate and fast finality through efficient message aggregation [438]. However, it is currently not supported in Ethereum Besu, and integrating it would require significant architectural changes.

Future Potential: If Besu or another enterprise Ethereum client adds support, HotStuff could dramatically increase DEIFP's scalability.

In summary, Ethereum Besu is a secure, enterprise-grade blockchain platform ideal for permissioned networks like DEIFP. By adopting Clique PoA, DEIFP benefits from low-latency, controlled consensus suited to a consortium of trusted public institutions. The protocol ensures key blockchain security properties such as safety, liveness, immutability, and accountability, aligning with theoretical underpinnings. If DEIFP is expanded to include more diverse stakeholders or jurisdictions, IBFT 2.0 is a suitable alternative that can ensure Byzantine fault tolerance without compromising on performance. The careful selection and monitoring of validator nodes reinforced by cryptographic signatures and observer oversight provides a robust trust infrastructure tailored for public sector antifraud efforts.

# Chapter 6

# Design of the decentralized employment integrity and fraud prevention framework (DEIFP)

## 6.1 Overview

This chapter introduces the Decentralized Employment Integrity and Fraud Prevention (DEIFP) Framework designed to use Ethereum Besu-based blockchain technology. This chapter explains the design science methodology and outlines the conceptual design of the DEIFP Framework, detailing its objectives, key components, and implementation strategy. It explains how blockchain's key features: decentralization, immutability, transparency, and security, can be leveraged to reduce ghost worker fraud in Nigeria's public sector.

## 6.2 Objectives of the framework

The DEIFP framework aims to accomplish five objectives that tackle the problems associated with ghost worker fraud in public sector employment systems. These objectives enhance data integrity, ensure accountability, enable stakeholders to work together, and enhance access control. These objectives are essential for building a strong framework that could curb fraud and make sure that employment records remain accurate.

### 6.2.1 Enhancing data integrity

The DEIFP Framework's primary objective is to assure employee data integrity by means of accurate, tamper-proof employment records that accurately depict the real status of employment in government entities. Data integrity refers to data's accuracy, consistency, and reliability throughout its existence [192]. Because data recorded on the blockchain ledger cannot be altered without detection, individual attempts at fraud are virtually impossible; any unauthorized insertion would require collusion among multiple validators. Immutable blockchain records provide a clear, verifiable history of employment data that authorized parties may access and verify, decreasing the possibility of fraud [368]. This feature of blockchain technology would provide a high degree of data integrity.

**Immutability and transparency:** Blockchain's immutability would guarantee that once validated records entered into the system, they stay permanently recorded [12]. Any update to an employee's data sets an alarm or flag for inspection, therefore guaranteeing that illegal modifications cannot go unnoticed. This transparency fosters great system trust, which is necessary for public sector accountability.

### 6.2.2 Facilitating strong verification process

The ability to verify employee data in real time is an important feature of the DEIFP Framework. This is critical for discovering inconsistencies such as ghost employees, and duplicate records. The DEIFP Framework ensures that personnel records are confirmed against verified agencies by adding blockchain technologies into current government systems.

### 6.2.3 Increasing stakeholder collaboration

The DEIFP Framework is intended to improve collaboration among different parties in the employment verification process. Decentralisation lets several stakeholders to independently verify employment records. The distributed structure of blockchain lets cross-agency cooperation and data sharing possible instead of depending on one agency

to maintain and validate data, therefore enhancing accountability and lowering the possibility of fraud going unnoticed.

A detailed stakeholder analysis was conducted to identify the roles, power, interests, and influence of all actors involved in the employment validation and employment process. The analysis adopted a power–interest grid [123], complemented by stakeholder salience theory [337] to prioritise engagement.

Key stakeholder groups include Validators which consist of core agencies like the IPPIS office, Office of the Accountant General of the Federation, and the Central Bank of Nigeria (CBN). These hold high power and high interest, as they directly validate employee data. The Federal Character Commission is a federal executive body established by Act No. 34 of 1996 and reinforced by Sections 14 and 153 of the 1999 Constitution [109]. Its primary mandate is to promote fairness and equity in the distribution of public posts and socio-economic infrastructure across Nigeria's diverse ethnic and regional groups [109]. Some of the key functions are to ensure equitable representation of states and ethnic groups in federal appointments and employment, and also to monitor recruitment processes in Ministries, Departments, and Agencies (MDAs).

The Central Bank of Nigeria is the apex monetary authority in Nigeria, established under the CBN Act of 1958 and currently governed by the CBN Act of 2007. It is responsible for monetary policy formulation and implementation, financial system stability, and currency issuance. Some of the key functions are to issue and regulates the Nigerian currency (Naira). Also, to act as banker and financial adviser to the federal government.

The Head of the Civil Service of the Federation is the topmost civil servant in Nigeria, responsible for the administration and coordination of the federal civil service. The office oversees employee participation, which significantly impacts organizational performance through involvement, engagement, and empowerment [299] and operates under the Office of the Secretary to the Government of the Federation and plays a central role in public service reforms. Some of the key functions are to coordinates human resource management across MDAs. Also, to ensure adherence to rules, ethics,

and standards in the civil service.

The Office of the Accountant General of the Federation is responsible for the management and control of federal government finances. It operates under the Federal Ministry of Finance and ensures the accountability and transparency of public funds [297]. Some of the key functions include overseeing payroll systems such as the Integrated Payroll and Personnel Information System (IPPIS) and conducting internal audits and ensures compliance with financial regulations.

Observers are agencies such as the Economic and Financial Crimes Commission (EFCC), Independent Corrupt Practices Commission (ICPC), judiciary bodies and the police. They have high power but moderate operational interest, serving mainly as auditors and overseers.

The end-users such as HR officers and payroll administrators within ministries and agencies. They have high interest but lower systemic power; they interact daily with data entry and validation processes. While the technical stakeholders such as the IT teams, blockchain developers are responsible for maintaining, deploying, and updating the system.

This analysis directly influenced design choices. For instance, the framework adopts a permissioned consortium blockchain where only validated government agencies can propose or approve transactions. Observers were included as non-validating nodes to provide independent oversight, reducing the risk of collusion by validators [346]. The analysis also identified training needs among end-users, shaping plans for capacity-building and usability improvements.

**Independent validation:** Stakeholders including CBN, FCC, and IPPIS can independently access and validate staff records therefore guaranteeing no single point of control. Blockchain's transparency lets any participant independently trust the data without depending on centralised administrators.

**Shared responsibility for fraud prevention:** The framework makes things clearer and makes sure that agencies all work together to prevent fraud. This is done by letting multiple parties validate employment information. This reduces the possibility of fraud

being undetectable, especially in large government organizations where internal control could be lacking [356].

### 6.2.4 Strengthening access control

Access control is an essential component of the DEIFP Framework, guaranteeing that only authorized workers can change employee data. The framework uses blockchain's smart contracts to ensure that data permission are securely controlled and that unauthorized access or manipulation is avoided.

**Smart contracts for automated validation:** Blockchain's smart contracts guarantee that data changes only occur if they satisfy pre-defined conditions, such verification from a specified number of stakeholders or data consistency checks, ensuring automated validation. By greatly reducing human error and manipulation, this automated validation procedure guarantees system integrity [60].

### 6.2.5 Encouraging reporting of irregularities

The DEIFP Framework would have a unique feedback system that lets workers and other stakeholders report problems or suspicious activities in the system. Transparency and immutability of blockchain guarantees that reports are auditable and tamper-proof, so enabling swift response should fraudulent activity be found.

**Anonymous reporting:** Employees and other interested parties can anonymously report fraud or disparities knowing that the system will safeguard their identity and guarantees the investigation of the claim. Blockchain's transparency guarantees that a report is validated and acted upon by the pertinent authorities.

**Real-Time monitoring and alerts:** The feedback system enables real-time observation of reported irregularities as well. Alerting stakeholders automatically and flagging suspicious records quickly helps to ensure that fraud is discovered as early as possible.

### 6.2.6 Conclusions

The framework's objectives include enhancing data integrity, enabling strong verification process, promoting collaboration among stakeholders, strengthening access control, and encouraging reporting of irregularities are all designed to minimise the possibility for fraudulent conduct and guarantee that the system stays transparent and accountable.

## 6.3 Key components of the DEIFP framework

The DEIFP Framework aims to combat ghost worker fraud in public sector payroll and employement systems. The framework has five fundamental components that ensure the integrity, security, and effectiveness of the employment data verification process. Together, these elements offer a complete solution for reducing fraud and enhancing accountability and transparency in employment systems. The five key components of the framework are:

1. Decentralized Data Sharing
2. Strong Verification process
3. Stakeholder Collaboration
4. Access Control and Security
5. Feedback Mechanism

Every element is vital in allowing the DEIFP Framework to be a strong, tamper-proof, effective tool for reducing ghost worker fraud and guaranteeing employment data integrity.

### 6.3.1 Decentralized data sharing

Decentralized data sharing is a fundamental component of the DEIFP Framework enabled by blockchain technology. In a decentralized system, data is disseminated among

numerous stakeholders, thereby preventing any single party from obtaining complete control over the payroll or employment records [329]. By incorporating many independent actors in the validation process, this strategy ensures transparency, reduces the chance of fraud, and increases accountability [329]. Studies have underlined how important strong validation systems are to maintaining data integrity and transperancy in many different fields. Multiple independent parties involved in the validation process help to lower fraud risks and enhance accountability [416].

**Blockchain's role in decentralization:** Blockchain's distributed nature guarantees that no one entity or agency may change the data without being detected. Whether a government agency, regulatory body, or security agency, every stakeholder engaged in the job verification process has access to a shared ledger including employment records. This shared ledger is always being updated as new information is verified and validated. It gives a full, up-to-date state of the employment record system. Once information is added to the blockchain, it can't be changed without leaving a trail for auditing. For example, if a new employee data is added to the shared blockchain ledger for validation, agencies independently verify and validate. This ensures no single agency has the ability to alter records in isolation, greatly reducing the possibility of ghost worker fraud.

**Preventing centralized fraud:** People working in the same department or agency could change records, which is one of the problems with traditional centralised payment systems. These systems frequently rely on manual operations, which leads to inefficiencies and higher fraud risks [384]. The centralised nature of these systems establishes a single point of failure that corrupt actors may exploit. The decentralized strategy of the DEIFP Framework, on the other hand, gets rid of this risk by giving validation and recording responsibilities to a number of separate stakeholders. With more than one level of oversight, any mistakes or fake records are more likely to be found quickly. For instance, in cases like the Nigeria Police Force payroll fraud in August 2024, which involved 4,190 ex-employees still receiving salaries despite being inactive [107], a decentralized system would have ensured real-time updates and cross-agency verification, immediately flagging any discrepancies.

**Enhanced transparency:** Blockchain enables transparent, independent verification of employment data by all parties involved. Because blockchain keeps an immutable record of all data transactions, all changes to the data are permanently documented and made publicly available to authorized parties. In this manner, each participant is held accountable for their actions. The distributed system also offers an audit trail whereby every change made to documents could be followed back to the party responsible.

### 6.3.2 Verification

The DEIFP Framework's strong verification process is another critical element that ensures the instantaneous and continuous verification of employee records across numerous agencies. This feature ensures that all new entries or modifications are promptly verified to prevent the inclusion of fraudulent or ghost workers into the system.

**Automated cross-verification:** The information of the newly hired employee is instantly checked and validated against several agencies, including IPPIS, CBN etc., as they are captured into the system. Real-time differences such as ghost employees, duplicate records, or inconsistent employment status are found and marked for quick probe.

**Blockchain's role in real-time validation:** The blockchain's decentralized nature allows for real-time updates across all network copies, ensuring data integrity and immutability [161]. New employee data entered is cryptographically confirmed by system validators. Transactions are validated quickly, but finality depends on the consensus mechanism's liveness and safety parameters; typically, a transaction is considered final after multiple validators sign and sufficient subsequent blocks confirm its permanence. This acknowledges that while blockchain adds data quickly, real-world finality is not strictly instant and depends on consensus configuration. But in traditional systems, it take weeks or months to verify records, this gets rid of the gaps that happen so that fraudulent entries can go unnoticed.

**Fraud prevention:** Real-time processing is required for timely fraud detection, but implementation problems include data quality assurance and privacy concerns. By analysing physiological and behavioural indicators, including real-time human detection into identity authentication enhances security [272]. This proactive approach to fraud identification decreases the likelihood of significant financial losses.

### 6.3.3 Stakeholder collaboration

Collaboration between stakeholders is an important part of the DEIFP Framework. The framework enables different stakeholders, such as the IPPIS, CBN etc to independently evaluate personnel records by decentralising the data validation process. This coordinated effort provides data transparency and early detection of fraud through independent validation from several stakeholders.

**Improved trust and accountability:** Involving several independent bodies for the verification process helps the DEIFP Framework promote accountability and cooperation. Blockchain-based audit trails improve the security, transparency, and reliability of enterprise systems. These solutions utilize the tamper-proof nature of blockchain to establish immutable records of system events, thereby guaranteeing data integrity and provenance [330] [12].

**Shared responsibility for fraud prevention:** The framework promotes shared responsibility for fraud prevention, ensuring that no single entity has complete control of the job verification process. Recent research emphasizes the significance of collaborative approaches in fraud prevention. Ilias et al. revealed that risk assessment, control actions, and information sharing have a good impact on fraud prevention in the public sector [185].

### 6.3.4 Access control and security

Access control and security are critical to ensuring the integrity of the DEIFP Framework. Blockchain technology can provide Role-Based Access Control (RBAC) in many

different contexts successfully [106]. The implementation of RBAC methods on blockchain platforms improves access control policy security, auditability, and transparency [106] [288]. Enforcing RBAC regulations depends mostly on smart contracts, which guarantee that only authorized users may access or change particular data [323]. Blockchain-based RBAC systems have benefits include preventing illegal access, protecting data integrity, and providing dynamic policy updates based on user context, including location [106] [288]. Various blockchain systems including Ethereum and EOS have been investigated for RBAC implementation. EOS shows potential in terms of scalability, cost-effectiveness, and performance [323].

**Role-Based Permissions:** The DEIFP framework is responsible for assigning various permissions according to roles. For instance, staff from the HoS can add employee records, but they are unable to change the data once it has been added to the blockchain. Auditors and other agencies, such as the Police, the Judiciary, or the EFCC, have access to the data as well, but they are impossible to make any changes to them. The possibility of fraud is decreased as a result of this measure, which ensures that data is only modified by those who possess the necessary permissions.

**Encryption and data protection:** Blockchain ensures that sensitive employee data is encrypted both at rest and in transit, protecting it from unauthorized access. The blockchain technology makes use of sophisticated cryptographic methods to guarantee the privacy and security of transactions. Each transaction is encrypted and connected to previous records, which results in the creation of an immutable chain on the blockchain [303]. A number of essential components, including mathematical hash functions, elliptic curve cryptography, and zero-knowledge proofs, are essential to the solid security that blockchain technology provides [417].

**Audit trail:** Blockchain immutable ledger makes it possible to provide a comprehensive audit trail of any modifications made to the system. The technology provides ledgers that are both immutable and transparent, which improves the traceability, accountability, and security of a wide range of applications. As a result of its distributed

nature, there is no longer a requirement for trusted intermediaries, which makes it possible for peer-to-peer transactions to take place directly [41]. Blockchain-based supply chain management solutions such as OriginChain provide tamper-proof traceability information as well as automated regulatory compliance checks [232]. The technology has a substantial influence on auditing since it creates a triple-entry accounting system in which transactions are immutable, timestamped, and encrypted in real time [66]. The provision of this function guarantees a comprehensive and traceable audit trail, which is essential for the maintenance of accountability.

### 6.3.5 Feedback mechanism

The feedback mechanism enables employees and stakeholders to report irregularities, fraud, or suspicious activity. This component is essential for maintaining the integrity of the DEIFP Framework by facilitating the early detection of fraud and irregularities.

**Anonymous reporting:** Employees and stakeholders have the ability to report any issues in an anonymous manner, while also assuring protection for those who blow the whistle and encouraging a culture of transparency.

**Encouraging reporting:** A incentive system can be integrated into the framework to urge employees and stakeholders to report fraudulent activity. This increases the likelihood that any abnormalities will be discovered as soon as they occur.

## 6.4 Design

This section details the design of the framework. First, the methodology is thoroughly discussed in subsection 6.4.1 and subsection 6.4.2, highlighting and explaining the Design Science Approach, which was the type of method used. Secondly, the architectural design that could address public sector employment issues was described.

### 6.4.1 Methodology

Conceptual designs have been the main focus of typical early research attempts [237]. As part of these conceptual designs, architectural plans and methods are often shown as pseudocode. Some studies [243] have also used queuing theory for simulation model of blockchain systems. Alternatively, scholars have undertaken investigations into the potential applications of recently developed blockchains through experimentation [14]. Although Ethereum operates as a public blockchain, it is possible to design and implement programs in Ethereum that limit access solely to authenticated users [375]. Another approach that can be taken is through Hyperledger projects, such as Hyperledger Fabric and Ethereum Besu [174] designing and implementing Hyperledger Fabric blockchain for securing the edge of IoTs [30], designing blockchain application for health care solution [2] who designed blockchain-based peer-to-peer trading platform, and [399] blockchain for drug traceability. These projects offer permissioned blockchain infrastructures that are appropriate for use within government and organizations. Out of these options, the most pragmatic strategies involve the utilization of Hyperledger projects or Ethereum smart contracts, both of which have undergone rigorous testing and implementation [18]. Hyperledger projects are designed to support enterprise-level business-to-business applications, whereas Ethereum hosts a multitude of functional projects. In the pursuit of developing decentralized applications for client utilization, Ethereum smart contracts are commonly utilized by development companies and developers [240].

#### Design science methodology

Design Science is a highly effective methodology for enhancing processes, since it is a problem-solving approach that aims to enhance human comprehension through the development of creative products [85]. Design process and engineering utilize modelling is a key component [253]. Design research emerged as an academic discipline in 1966 with the establishment of the Design Research Society [342]. Despite being frequently overlooked, design plays a crucial role in various fields. The society's founders revealed

the necessity of this new field of study by observing that design appeared to have a distinct theoretical base [342], which included "designerly ways of knowing" [100] and "a designerly way of thinking and communicating" [33]. This foundation warranted further investigation and analysis.

The primary objective of design research, in its original emergence, was to formulate a theory pertaining to the process or phenomena of creating man-made objects and artefacts [407]. The primary aim of design science research is to enhance the existing technological and scientific knowledge repositories by developing novel artefacts that effectively address challenges. The part of this study adopts the Design Science approach, which encompasses six fundamental actions:

**Problem identification and motivation** The first stage was to conduct a thorough review and analysis of the IPPIS in section 2.6 to identify the problems relating to ghost worker fraud, with a focus on how the system accommodates ghost worker fraud and the need for a transparent and verifiable system.

**Defining the objectives** The proposed blockchain-based solution is accompanied by well-defined objectives that were established in the previous chapters of this study, see subsection 1.3.1. These objectives guide the rest of the study process.

**Designing and developing** In the design phase in section 6.5, the proposed solution is conceptualised and architecturally planned and developed.

**Demonstration** The functioning of the produced solution is demonstrated through a demonstration, with an emphasis placed on how it addresses the difficulties that have been highlighted in the method of employment.

**Evaluation** An in-depth analysis of the proposed solution is carried out in Chapters Chapter 7 and Chapter 8. The acceptance of the framework, its security features, and its capacity to improve transparency and verification in the employment process are all evaluated as part of the process.

**Communication** Making the findings of the research public is the final step in the process. Not only does this include the presenting of evaluation outcomes, but

it also includes the documentation of the design and development process. Communication is employed in order to make sure that the research offers significant insights to the professional and academic communities.

The subsequent section provides an explanation of the mapping process.

### 6.4.2 Mapping design science approach with this study

The Figure 6.1 depicts the sequential and systematic strategy that was adopted in this research, which adhered to the principles of design science. Beginning with the identification of the problem, which is the widespread problem of ghost worker fraud, each stage in the picture reflects an important element in the research process. In the first step it establishes the reason for the investigation and to emphasize the necessity of finding a solution. The second step entails identifying clear objectives, with a particular emphasis on utilizing blockchain technology to eradicate this type of fraudulent activity. In the third stage, it enters the design and development phase, which is where Ethereum Besu is utilized to develop the blockchain framework. Demonstration is the fourth stage where real world cases were utilized to demonstrate the functionality of the system in a setting that is applicable to real-world situations.

The evaluation phase as the fifth stage is an essential part of the process, and it involves the use of real world case studies and quantitative survey where the perceptions of government employees and blockchain experts are captured to evaluate of the proposed DEIFP framework to ensure that it satisfies the necessary requirements of both efficiency and transparency. In the final step, the communication phase, the findings of the research are disseminated to the wider community through scholarly publications and professional presentations. Through the utilization of this strategy, every stage of the investigation builds upon the one that came before it, resulting in a validated proposed solution to the problem of ghost worker fraud.

#### Problem identification and motivation

The DEIFP framework specifically focuses on enhancing data security and transparency in the employment process. The underlying rationale is to augment transparency and

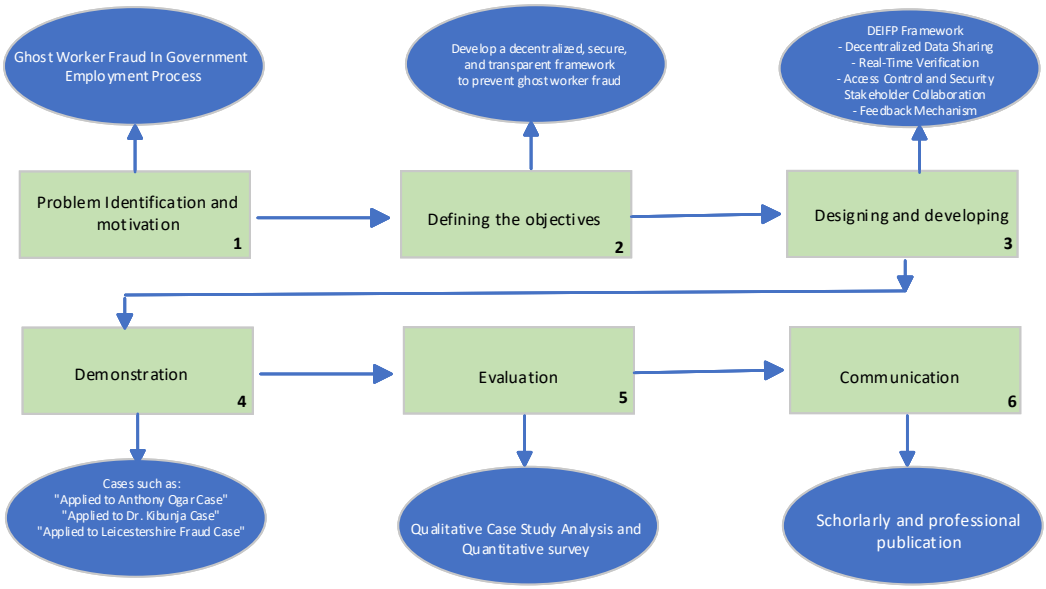


Figure 6.1: Design Science Approach Mapped with the Proposed Solution; Green area indicating key actions while blue area portraying the proposed solution

dependability in the process of approving newly hired personnel. Thorough literature view was conducted in this regard highlighting the problems of ghost worker fraud in Nigeria and elsewhere, see section 1.2. Besides establishing existence of ghost worker fraud through recent literature, survey on the perception of ghost worker fraud existing in the IPPIS employment process in 2021 was conducted which is one of the objectives of this study, see Chapter 4. The outcome shows the existence of ghost worker fraud in IPPIS and the need to curb it.

### Defining the objectives

The primary aim of this study is to identify a blockchain-based solution that could improve transparency and data integrity within the employment process in Nigeria. It is necessary to set explicit objectives for the creation of a system that is both secure and transparent. The objectives were enumerated in subsection 1.3.1.

**Designing and developing**

The combination of Ethereum Solidity and Ethereum Besu is proposed to be utilized in the process of developing the solution. These technologies are the foundation of the DEIFP framework, which is designed to capture, approve, validate, and manage the process of hiring new employees. During the design phase, conceptual DEIFP framework for the blockchain solution was developed, which included essential elements including smart contracts for verifying employment, consensus mechanisms for approval workflows, and data encryption for safeguarding privacy as depicted in Figure 6.2. Smart Contracts should be written with the purpose of automating the processes of verifying employees, and guaranteeing that only legitimate employees are included in the payroll.

**Demonstration**

The Demonstration phase in this study followed the principles of Peffers et al. Design Science Research Methodology (DSRM) [310]. Rather than implementing a full-scale technical prototype, the focus was on conceptually demonstrating the feasibility and practical value of the proposed Decentralised Employment Integrity and Fraud Prevention (DEIFP) framework. The demonstration was carried out through:

1. Scholarly dissemination and feedback: The framework was presented at academic conferences and seminars, as well as internally among members of my research group. These discussions provided critical and constructive feedback regarding design assumptions, potential challenges in stakeholder adoption, and practical considerations for integrating blockchain in public payroll systems.

2. Conceptual design: Rather than coding and deploying smart contracts, a diagram that illustrated how DEIFP would operate in practice showing was developed, for instance, how the multiple agencies could act as validators in a permissioned blockchain network, as shown in Figure 6.2.

3. Case study evaluation: As part of the evaluation phase, real-world high-profile cases of ghost worker fraud were used to conceptually demonstrate how DEIFP

could mitigate similar fraud vectors. While this was primarily evaluative, it also served a demonstration function by highlighting the framework's practical applicability to real fraud scenarios.

Lessons learned from this demonstration phase included:

1. The need for clear governance structures and stakeholder role definitions to ensure validator independence and accountability.

2. The practical challenge of integrating decentralized frameworks with existing centralized HR databases (IPPIS), which may vary in data quality and structure.

3. Feedback emphasized that while blockchain can technically enhance data integrity and traceability, organizational buy-in and inter-agency cooperation are critical determinants of real-world success.

Overall, the demonstration phase helped refine the DEIFP framework conceptually, ensuring it was not only technically sound but also practically relevant and aligned with stakeholder needs, even though no working software prototype was developed or deployed.

**Evaluation**

The DEIFP framework was evaluated using both qualitative and quantitative methodologies to ensure a thorough review. The qualitative evaluation involved the analysis of real-world fraud cases, where vulnerabilities in existing payroll systems were identified, and the potential impact of the DEIFP framework was considered, see Chapter 7. The quantitative evaluation, which was carried out via survey, gathered data from government employees and some blockchain experts to assess their perceptions of the effectiveness of IPPIS and the DEIFP framework, see Chapter 8. Both techniques provided useful insights into the DEIFP framework's strengths and flaws, combining real-world examples with empirical data to assess its viability in combating ghost worker fraud.

**Communication**

After completing the research work outlined in the previous steps, the findings are now being disseminated through various scholarly and professional channels. During the course of this research, progress updates and preliminary findings were regularly shared at the weekly meetings of the Strathclyde Cyber Security Group (StrathCyber) in the department, which comprises over forty staff members and PhD students [378]. These presentations provided valuable feedback and insights that helped refine the research.

In addition to internal presentations, I have actively participated in workshops and conferences and published research papers in academic journals. I presented the paper `Potentials of Blockchain Technology for Payroll Systems`, check [55] at the Southern Association for Information Systems (SAIS) Conference, which fosters close interaction between presenters and attendees, ranging from doctoral students to senior faculty. I also attended an ACM conference in the United States, where I presented `Curbing Ghost Worker Fraud In Developing Countries Using Consortium Blockchain` check [56]. The paper is published in the ACM Digital Library.

Furthermore, I presented a poster titled `Blockchain Framework for Enhancing Employment Integrity to Curb Ghost Worker Fraud` at the Academic Centres of Excellence in Cyber Security Research (ACE-CSR) Conference, Lancaster University. These efforts aim to share the insights and lessons learned from the development of the blockchain solution to address ghost worker fraud.

**Key refinements that emerged from this stage included:** Validator and observer structure: The original design envisioned a network with a fixed number of validators. Feedback emphasized the importance of enhancing transparency and accountability by introducing non-validating observer nodes (e.g., EFCC, judiciary) to monitor activities. This aligns with recommendations in blockchain security literature.

**Lessons learned:** The Communication stage underscored the value of iterative stakeholder engagement in refining on technical aspects of the framework (e.g., consensus

design, validator structure). This iterative refinement process reflects the guidance of Chamberlain and Bowen, highlighting that design artefacts become more robust and contextually appropriate when shaped by continuous feedback [88].

### 6.4.3 Conclusion

This research adopts the Design Science Concept. This approach was used for the design of the DEIFP framework. The method ensures the effectiveness, efficiency, and robustness of the proposed solution through adherence to a systematic process that includes problem identification, solution design, development, evaluation, iteration, demonstration, and communication.

## 6.5 Architectural design

The design of the DEIFP framework shows how different components are structured and how they interact with each other, as shown in Figure 6.2. The architecture includes the Head of Service (HoS), Federal Character Commission (FCC), IPPIS, CBN, and related Ministries. These entities validate and verify transactions as blockchain nodes. The network includes non-validating peers for wider involvement without compromising security. The framework employs Inteplanary File System (IPFS) for decentralized storage to securely data, including employment records and documents. Decentralization is a fundamental element of this design, as it disperses control and data storage among numerous nodes, thus eliminating individual points of failure and minimizing the possibility of unauthorized manipulation. The system utilizes decentralized storage using IPFS to securely maintain employment records, allowing access or modification only through consensus among various validating institutions.

This decentralized strategy is essential to the anti-fraud idea covered in section 2.5 which highlight frauds and corrupt practises involving ghost workers. The blockchain's capacity to document each transaction in an immutable manner, along with the automation facilitated by smart contracts, ensures that any effort to introduce fraudulent data or manipulate existing records is promptly detectable and confirmable throughout

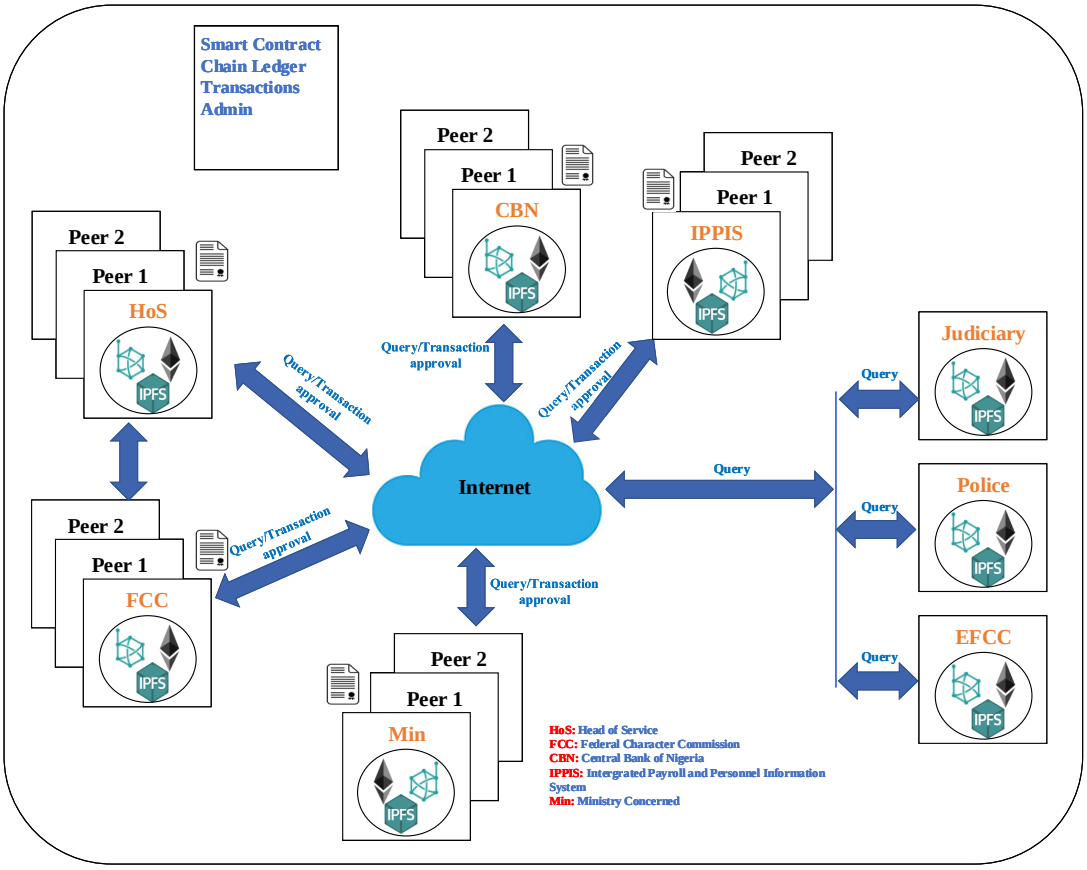


Figure 6.2: Decentralized Employment Integrity and Fraud Prevention (DEIFP)

the network, thereby preserving the integrity of the employment process. Adding a new employee or updating records starts the workflow in this design. Smart contracts verify the conditions and update the chain ledger for this transaction.

HoS, FCC, IPPIS, CBN, and Ministries validate the transaction through a consensus procedure to ensure data updates are authorized. A verified transaction is permanently recorded on the blockchain, and necessary documents are kept on IPFS for all authorized nodes. Admins manage rights and security protocols on the network. The Internet connects these components, allowing real-time data sharing and verification to combat ghost worker fraud by maintaining accurate and transparent employment records. Some components, including the network nodes and topology, data storage architecture, and integration points with existing systems are discussed:

### 6.5.1 Data storage architecture with interplanetary file system (IPFS)

In the blockchain framework, data is stored using a distributed ledger model, where events are recorded in blocks in the order they happened. The blockchain keeps permanent records of employee data, such as personal details and the state of their validation. The Interplanetary File System (IPFS) would be used to store data by the Private Ethereum Besu blockchain structure. IPFS is a peer-to-peer distributed file system that connects all computers to a single set of files [278]. It is a content-addressed block store model with a high throughput. It uses content-addressed hyperlinks and combines technologies like Distributed Hash Tables (DHT), incentivized block exchange, and self-certifying namespaces.

Naz et al. developed this framework that utilizes blockchain technology to ensure secure sharing and delivery of digital assets. The framework ensures the authenticity and integrity of data for clients while also providing a reliable business platform for data owners [278]. In Figure 6.3, the Owner uploads data to IPFS and uses Shamir's Secret Sharing to encrypt hashes from the data. After that, the customers make a request for data, the workers verify their identity, and then they download the data from IPFS after making a payment deposit. Arbitrators are responsible for resolving disagreements between clients and the system in relation to data downloads. The system also incorporates a review mechanism, which allows customers to provide feedback on both the data and the owner.

IPFS does not have a single point of failure, and network sites do not have to trust each other. This makes the system strong and resistant to attacks or failures. Unlike traditional cloud storage solutions that use centralized servers, IPFS spreads data across many places around the world. This makes data more available and fault-tolerant. In the context of this research, IPFS serves as the primary storage mechanism for files. When a file is added to IPFS, it is given a unique cryptographic hash string that tells the system where it is. Users can get the file by using this hash string as a unique name, which works like a Uniform Resource Locator (URL) on the Web.

Users can only access encrypted files kept on IPFS if they follow the rules set by

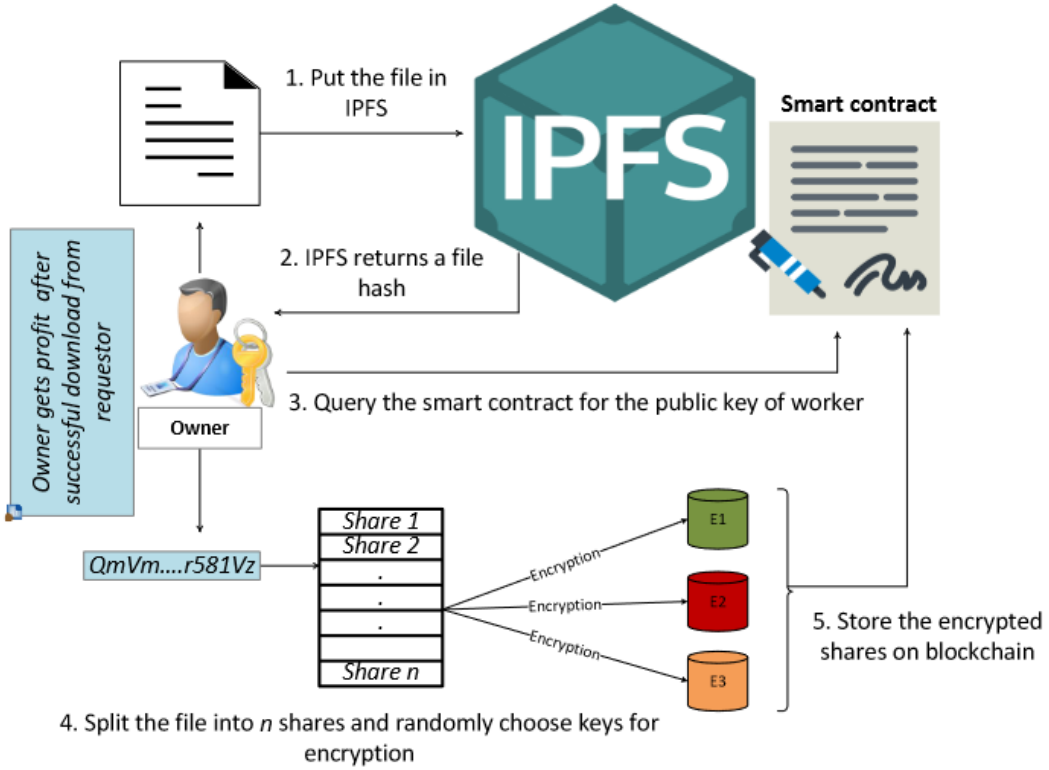


Figure 6.3: Data Sharing On IPFS By Owner [278]

the owner of the data as shown in Figure 6.3. Files on IPFS are encrypted before being uploaded, and only users with the necessary decryption keys can access them. The file's location (hash) is immutably kept on the blockchain, and smart contracts enforce access control by limiting who can acquire the file hash and decryption key. This method ensures confidentiality by encrypting the file, allowing only those with the key to view it. It also ensures data integrity and immutability, as any changes to the file generate a different hash that does not match the one saved on the blockchain. This technique enables the efficient, scalable, and secure processing of huge files by combining blockchain's strong access control with IPFS's distributed storage.

### 6.5.2 Why integrate IPFS, and how is security preserved

#### Rationale for integrating IPFS

Storing large files directly on a blockchain is technically feasible but impractical and inefficient. As highlighted by Zheng et al., blockchain networks are optimised for small, verifiable data (such as hashes and transaction records) rather than large binary files like employment records, certificates, and scanned documents. Storing these directly on-chain would lead to high storage costs, increased block size, and reduced scalability [444]. InterPlanetary File System (IPFS) offers a complementary solution by providing a distributed, content-addressed storage network. Instead of storing the documents themselves on the blockchain, the DEIFP framework will store only the cryptographic content hashes (e.g., Merkle roots) of files that reside in IPFS. This design ensures that the integrity of documents is cryptographically verifiable, meaning, any alteration to the content results in a different hash, which would no longer match the hash recorded on the blockchain. Also, storage is distributed across multiple nodes, reducing single points of failure and improving resilience.

#### How security is preserved

**Immutable hash anchoring:** The blockchain stores immutable records of each document's content hash. This ensures that any tampering or replacement of files can be detected.

**Distributed storage:** IPFS nodes store the actual documents. The decentralized architecture of IPFS protects against data loss due to the failure of any single node.

**Tamper detection:** If someone modifies a file in IPFS, the new content generates a different hash. Since the blockchain holds the original hash, discrepancies become immediately apparent.

### Limitations and considerations

**Content deletion risk:** IPFS itself does not guarantee permanent availability. If no node continues to "pin" a file, it could become unavailable. Thus, organizational governance and redundancy strategies are required.

**Complementary immutability:** True immutability comes from the combination: blockchain ensures the integrity of document hashes, while IPFS offers distributed content storage. As noted by Patel, IPFS alone cannot guarantee data permanence without adequate replication [307].

### Why documents not directly stored on-chain

**Cost:** Blockchain storage is resource-intensive; each byte of data stored requires network consensus and occupies space in every full node's copy of the ledger [304].

**Scalability:** Storing large files on-chain would drastically slow block propagation and reduce network performance [167].

**Efficiency:** On-chain design is best suited for metadata and references, while off-chain systems handle bulk data [439]. Hybrid architectures combining on-chain and off-chain systems offer a balanced approach, with on-chain components managing metadata, verification data, and permissions, while off-chain systems handle bulk data storage [439] [255].

### Conclusion

By integrating IPFS with blockchain, the DEIFP framework balances decentralisation, data integrity, scalability, and operational efficiency. The blockchain layer guarantees that records cannot be tampered with undetected, while IPFS enables efficient and distributed storage of larger documents—ensuring both transparency and practicality in combating ghost worker fraud.

## 6.6 Implementation strategy for the DEIFP framework

This section provides a plan to implement the proposed framework. Strategy to implement both technical progress and the ability of parties to work together as a team is presented here.

### 6.6.1 Stakeholder involvement and collaboration

The DEIFP framework will depend on efficient communication, cooperation, and coordination among various stakeholders—government agencies, regulatory bodies, security organizations, and technology providers.

**Government agencies:** The validation process would involve important government organizations like the CBN, FCC, and IPPIS. These organizations have to align their activities with the distributed structure of the DEIFP Framework and connect their current systems with blockchain technologies.

**Regulatory bodies:** Auditors and compliance bodies among other regulatory entities will be assigned to make sure the structure follows legal norms including public sector policies and data privacy legislation. They will be in charge of ensuring the framework's compliance, transparency, and security throughout its implementation.

**Security Agencies:** The Nigerian Police Force and the EFCC, among others, would be crucial in looking into any possible fraud that is discovered using the framework. These entities will react fast to fraudulent activity using the strong verification process and feedback systems of the framework.

**Technology providers:** To design, implement, and manage the blockchain infrastructure for the DEIFP Framework, blockchain developers and IT specialists will be needed. They will also make sure the public sector employment systems adequately incorporate blockchain decentralisation, security, and real-time validation features.

### 6.6.2 Technical development and integration

Ethereum Besu-based blockchain technology forms the foundation of the DEIFP Framework. Technical development include developing the blockchain infrastructure in line with current public sector systems such as the IPPIS via both building and integration. This section outlines the necessary technical steps.

**Blockchain infrastructure setup:** Setting up a strong blockchain infrastructure with Ethereum Besu comes first in the technical development phase. Using a permissioned blockchain, Ethereum Besu will be developed to build a private blockchain network allowing just authorized stakeholders to engage in the validation process. The blockchain will be built to securely store and manage employee data, with smart contracts automating the validation and approval process for new employee records.

**System integration:** The integration of the DEIFP Framework with present public sector systems may be one of the primary challenges in its deployment. IPPIS, which is used for payroll is an example of important system that need to be connected to the blockchain in order to provide strong verification process and validation across several agencies. In order to accomplish this, it may be necessary to create Application Programming Interfaces (APIs), which are interfaces that enable other systems to communicate with the blockchain network in a seamless manner.

**Data migration:** It is necessary to convert all of the user information that is now stored in legacy systems (such as IPPIS) to the blockchain system. During the migration process, it will be necessary to carefully organize this process in order to guarantee that all historical data is transferred accurately and that any inconsistencies in the data, such as ghost workers or duplicate entries, are detected and corrected.

**Security protocols:** It is absolutely necessary to put in place stringent security measures. It is necessary to configure encryption, smart contracts, and role-based access control (RBAC) in order to guarantee that only authorized users are able to add or change employee data after they have been created.

**Testing and quality assurance:** Prior to the complete deployment of the blockchain network and integrated systems, it is recommended that they be subjected to stringent testing. To begin with, unit testing of individual components (such as smart contracts and API integrations) should be began with. While integration testing to guarantee that the blockchain will interface appropriately with the legacy systems should follow. In addition, security testing that will ensure the system is resistant to hackers, fraud, and unauthorized access should be conducted. Further more, performance tests to make sure the blockchain can handle all the transactions that come from the employment process should be extensively performed.

### 6.6.3 Pilot testing and evaluation

After the blockchain infrastructure and system integrations are completed, the DEIFP Framework should be tested in a pilot program. Through pilot testing, potential problems could be identified, real-world data on the effectiveness of the system can be conducted, and stakeholder buy-in could be achieved.

**Pilot program design:** The prototype should be implemented within a limited number of government agencies that are responsible for employment management. It ought to involve a small sample of employee data, which will enable the framework to be tested under controlled conditions to ensure its effectiveness. During the pilot, the decentralized validation process will be put through its paces, strong verification mechanism will be assessed, and the feedback system will be utilized to identify any inconsistencies or fraudulent actions that may have occurred.

**Stakeholder feedback:** As part of the pilot program, it is important to collect feedback from key stakeholders, such as auditors, and employees, in order to identify any areas that could use improvement. It is essential to have this input in order to gain a knowledge of how the system functions under real-world settings and to guarantee that it satisfies the requirements of all parties involved.

**Evaluation metrics:** Before the pilot starts, success metrics should be set up. Examples of these include:

- Reduction in ghost worker fraud: This will reflect the reduction in the number of fraudulent payroll entries.
- Efficiency: Determine how much time is required for the verification of personnel data and the detection of fraudulent activity.
- Stakeholder satisfaction: Conduct a survey to determine the level of satisfaction that stakeholders have with the amount of transparency and usability that the system provides.
- Security incidents: Keep a record of any security breaches or incidents to ensure that the system is as strong as possible.

**Adjustments and optimisation:** Following the completion of the pilot program evaluation, the system ought to be modified in accordance with the comments and problems that have been detected. Among these are the implementation of technical enhancements, the enhancement of user interfaces, and the process of fine-tuning the feedback mechanism in order to guarantee improved fraud reporting.

### 6.6.4 Full-scale implementation

When the pilot phase of the DEIFP Framework has been successfully completed and any necessary adjustments have been made, the framework could then be rolled out for a comprehensive implementation. As part of this process, the blockchain system will be implemented across all key government departments, agencies, and ministries that are responsible for managing employment records.

**Scaling the blockchain network:** The infrastructure of the blockchain framework needs to be scaled up so that it can manage the complete amount of employment record across all government entities. This will most likely entail increasing network capac-

ity to ensure that the system can process thousands of records concurrently without interruption.

**Training and capacity building:** All stakeholders, including government officials, auditors, and security officers, are required to receive training on how to use the new blockchain system. Training programs ought to include instruction on the fundamentals of blockchain technology, the specifics of the DEIFP Framework, and the means by which to navigate the system in order to validate employee data and report illegal activity.

**Ongoing monitoring and support:** Following the implementation of the DEIFP Framework, it is essential to continuously monitor its operation in order to guarantee that it runs smoothly. Continuous technical assistance must be made available in order to fix any problems that may develop, and the framework should be audited on a regular basis in order to guarantee that it complies with all applicable legal norms and regulations pertaining to data protection.

**Public awareness:** Public awareness efforts ought to be carried out in order to promote acceptance and confidence in the new system. During these campaigns, the benefits of the framework, such as enhanced transparency and reduced fraud, can be explained to the general public as well as to the key players.

The proper implementation of the DEIFP Framework is crucial to tackling the ongoing problem of ghost worker fraud in the public sector. In order to achieve a seamless integration of the framework into government payroll systems, it is necessary to adopt a phased strategy that includes the participation of stakeholders, the development of technical components, pilot testing, and the deployment of the framework on a larger scale. This will result in an improved data integrity, enhanced strong verification process, and more coordination among key stakeholders, which will ultimately lead to a public sector employment system that is both more secure and more transparent. The DEIFP Framework has the potential to revolutionise the management of government employment procedures and reduce the financial losses that are connected with ghost

worker fraud, which could be accomplished through careful planning, testing, and continual improvement.

### 6.6.5 Conclusion

The DEIFP Framework seeks to address the widespread problem of ghost worker fraud by decentralising data validation and allowing many stakeholders—including government agencies, regulatory bodies, and security organizations—to get involved in the employment process and record keeping. This decentralized solution solves the vulnerabilities of traditional centralised payroll systems, where fraudulent acts are frequently carried out due to a lack of oversight or record manipulation by individuals in positions of power. The approach reduces the likelihood of fraudulent activity and increases accountability and transparency by distributing the task of data validation across a number of different entities.

The main goals of the framework are to enhance data integrity, facilitate reporting of abnormalities, collaborate with stakeholders, improve strong verification process, and control access. The implementation of blockchain technology assures that employee records are tamper-proof and unchangeable, resulting in great data security and confidence in the hiring process. There are several parts of the framework that work together to make a strong, effective system for stopping fraud. These include decentralized data sharing, strong verification process, stakeholder teamwork, access control and security, and the feedback mechanism. Through the utilisation of blockchain technology, the framework ensures that all employee data is recorded in a secure manner and in real time. This is accomplished by offering a procedure that is both auditable and transparent, which all stakeholders can have confidence in. Furthermore, the decentralized design of the system encourages collaboration among a number of different agencies, which in turn promotes transparency and accountability while also lowering the likelihood that fraudulent acts would go undetected.

The feedback mechanism is another critical component of the DEIFP Framework, allowing employees and stakeholders to anonymously report fraudulent or questionable activity. In addition, the implementation of a compensation system for reporting ab-

normalities would provide stakeholders with an additional incentive to engage in the process of preserving the integrity of the payroll system. In conclusion, the DEIFP Framework offers a novel approach for ensuring the integrity of employment in the public sector. This is especially important for nations such as Nigeria, where the matter of ghost worker fraud has been a big problem for a considerable amount of time. This framework has the potential to significantly reduce the risk of fraud, improve the efficiency of employment verification, and promote the accountability of government employment processes by utilising the characteristics of blockchain technology.

# Chapter 7

# Evaluation by case study

This chapter evaluates the effectiveness of the DEIFP in tackling ghost worker and employment fraud. The chapter highlights systemic weaknesses in payroll and employment verification processes by analysing high-profile fraud cases. These show the effects of weak access control, inadequate monitoring, and lack of cross-agency verification. The DEIFP framework is evaluated for mitigation and prevention of future fraud. The analysis shows how the DEIFP framework may improve employment processes and detect and prevent ghost worker fraud.

## 7.1 Justifying a case study approach

This first phase analysis is the qualitative approach, focusing on the examination of court case reports, news articles, and academic literature related to ghost worker fraud. The use of case studies as a methodological technique is well established in the literature, especially for investigating complicated phenomena in real-world contexts. Case studies provide researchers with rich, contextual data that could offer insights that are not easily captured through other research methodologies [76] [327] [77]. A case study technique is beneficial to the analysis of ghost worker fraud in the context of this study because it enables a comprehensive assessment of the ways in which various factors lead to fraudulent actions in employment process.

According to Simons, case study research is an effective method for conducting in-depth investigations of complicated problems that occur in real-world contexts [370]. One of its advantages is that it can accommodate a variety of data sources, such as observations, documents, and interviews, allowing researchers to fully comprehend complex occurrences [327] [370]. According to Griffiths and Ratnasari and Sudradjat case

studies have the ability to blend qualitative and quantitative data, which provides considerable flexibility in terms of research design and analysis [156] [327]. Because of this flexibility, case studies are especially useful for examining the interactive relationship between social, organizational, and technological elements that lead to fraudulent practices.

Successful case study research involves a balance of rigour, relevance, and pragmatism [105]. Developing precise concepts, specifying units and interactions, and carefully choosing instances are all recommended practices for positivist case studies in information systems [363]. Case studies are helpful in assessing information systems and tackling developing challenges. They offer insights into organizational difficulties and guide policy and practice [229]. This demonstrates how case studies can expose the operational issues organizations encounter when implementing fraud prevention frameworks, so offering insights that can guide policy and practice.

In addition, Witman offers a convincing illustration of how case studies can be used to investigate how banks adapted their compliance protocols in reaction to regulatory changes that demanded more robust authentication [427]. The research analyzed the responses of financial institutions to regulatory mandates for enhanced authentication, especially under time constraints. The qualitative insights obtained from the case studies identified critical weaknesses and emphasized recommended practices, demonstrating how case studies can assist organizations in improving their compliance efforts.

Case study research is regarded as a rigorous and valuable methodology in the social sciences, providing detailed insights into complicated phenomena [263] [285]. Even though case studies are criticised for being less generalizable and scientifically rigorous, they offer a comprehensive perspective on real-world situations by integrating various data collection techniques [285] [308]. This method is quite useful for developing and evaluating theories in organizational science [308]. Although case studies frequently use qualitative data, quantitative components can also be used [410]. The method's strength is its ability to investigate individual instances of social phenomena in depth, so contributing to our empirical understanding of social life [263]. However, methodological rigour is critical, especially in areas such as data collection and processing [410].

When executed correctly, case studies could offer valuable, context-specific insights that are indispensable for comprehending intricate social issues.

Case studies are useful for theory development because they allow researchers to create and refine theoretical frameworks based on practical data. This chapter seeks to add to the broader discussion on fraud prevention in public sector organizations by combining case study findings with theoretical development. In summary, case studies are a methodological approach that is strongly supported by the literature for examining complicated situations like ghost worker fraud.

## 7.2 Search Strategy and Data Sources

The case study evaluation aimed to understand the suitability and potential weaknesses of the DEIFP framework by analysing real-world cases of ghost worker fraud. A systematic literature search was conducted across multiple academic and grey literature databases to identify relevant cases. The following databases and sources were used:

1. Google Scholar: for broad access to academic articles, reports, and conference papers.

2. Scopus and Web of Science: to locate peer-reviewed papers, particularly in information systems and public administration.

3. IEEE Xplore: to find technical research on blockchain, fraud detection, and decentralised systems.

4. Government, News reports: including publications by Nigeria's Economic and Financial Crimes Commission (EFCC), Nigeria Newspapers, and Transparency International.

Keywords and search terms included: "ghost worker fraud in Nigeria", "public sector payroll fraud", "ghost employees in government payrolls", "employment fraud", "payroll fraud in public institutions", and "government fraud cases Nigeria". To ensure relevance to the contemporary policy and technological environment, only cases documented between 2010 and 2024 were considered. The search process initially yielded

approximately 38 papers and reports mentioning ghost worker, employment fraud or closely related payroll fraud. After screening for duplication and data sufficiency, 8 detailed cases were shortlisted for in-depth analysis.

**Inclusion and Exclusion Criteria**

The following criteria guided the selection of cases:

**Inclusion criteria:**

- Clear documentation of fraud mechanisms (e.g., how ghost workers were inserted into payroll systems).
- Occurrence between 2010 and 2024.
- Sufficient publicly available data to describe organisational context, vulnerabilities, and consequences.

**Exclusion criteria:**

- Cases without detailed explanations of fraud mechanisms.
- Incidents that could not be verified from at least two independent sources.
- Cases limited to non-payroll corruption (e.g., procurement fraud, bribery).

This approach ensured that each selected case contributed to evaluating the DEIFP framework against well-understood, documented fraud scenarios.

### 7.2.1 Rationale for the Period 2010–2024

Focusing on cases from 2010–2024 was deliberate for several reasons:

1. The period coincides with widespread digitalisation of payroll systems in Nigeria and comparable countries, increasing both complexity and opportunities for systemic fraud.

2. It reflects the era during which centralised payroll systems like Nigeria's IPPIS was widely adopted, making it highly relevant to this study.

3. Older cases might reflect outdated governance or technology contexts, potentially reducing the validity of the evaluation for today's public sector environments.

### 7.2.2 Case Selection and Justification

The initial search identified 38 potentially relevant documents. After applying the inclusion criteria and removing duplicates, 8 cases were selected for thematic analysis. They include:

1. Four cases came from Nigeria, reflecting high-profile ghost worker scandals in federal ministries, state governments, and educational institutions.

2. Four international cases were chosen to test whether the DEIFP framework could also address fraud in comparable contexts in Sub-Saharan Africa, Asia, and Latin America.

Although Nigerian cases were prioritized for their direct relevance to the national context in which the framework was conceived, broader cases were included to explore the generalizability and robustness of the framework beyond a single country.

#### Aggregating Nigerian Cases

Below, we justify why Nigerian ghost worker cases were considered collectively rather than analysed separately

1. Despite occurring in different institutions, these Nigerian cases largely share the same systemic weaknesses: heavy reliance on centralised payroll, and human-mediated data entry points.

2. Treating them as one cluster highlights common root causes targeted by the DEIFP framework, rather than repeating similar findings across several sub-cases.

3. In contrast, international cases were treated individually to compare how the framework's features might address fraud under different administrative and regulatory environments.

By concentrating on the most recent decade before this study, the analysis remains aligned with current practices and the intended context of the DEIFP framework. The method is consistent with approaches used in similar studies, such as in the research by Moreira et al., which employed case studies to evaluate cybersecurity frameworks in organizational contexts [262]. It is a case study a using a constructivist multicriteria methodology to evaluate the performance of NIST's cybersecurity framework controls.

Similarly, Fraser et al. utilized a multiple case study approach to assess the effectiveness of enterprise risk management frameworks, demonstrating the utility of case studies in exploring complex frameworks within real-world settings [141]. Additionally, Ocampo and E. E. Clark conducted case studies to evaluate sustainability frameworks in manufacturing, further illustrating the effectiveness of this methodology in examining the practical applications of theoretical constructs [291].

After the information was gathered, key details included the cause of the fraud, methods of execution, and systemic vulnerabilities. This data collection method aligns with the qualitative approach utilized by Kunhibava et al. who explored challenges in the use of regulatory technologies (RegTech) in Islamic and conventional financial markets using qualitative research approach through review of the B2C2 Ltd vs Quoine Pte Ltd. court case among others [212]. The study highlighted how qualitative insights from real-world cases could inform better regulatory practices and frameworks.

In addition, S. Grover uses a qualitative research process to analyze the competing meanings and perspectives of the various parties involved in a legal case [158]. The author conducted case studies approach using extracts from court filings of various parties in the Safford Unified School District vs Redding Supreme Court case. By analyzing the court rulings and reports he examined the text data to identify themes summarizing the diverse phenomenological perspectives of the parties.

Moreover, Beasley et al. examined financial statement fraud cases across three industries (technology, healthcare, financial services) from the late 1980s through the 1990s,

and compares the corporate governance of fraud companies to no-fraud benchmarks in those industries [48]. The research involved detailed analysis of financial reports and other legal documents. By employing a case study methodology, they could effectively highlight that that weak corporate governance mechanisms were associated with fraudulent financial reporting in technology, healthcare, and financial services industries. This approach demonstrates the value of qualitative data in assessing the practical implications of theoretical frameworks in real-world scenarios.

Furthermore, Rouse and Harrison emphasize the need of collecting multiple forms of data to enhance qualitative research findings [341]. The incorporation of diverse sources, such as legal documents and news reports, allows for a more holistic understanding of the phenomena under investigation. By integrating these different perspectives, researchers could create a comprehensive narrative that captures the complexities of issues like ghost worker fraud, thereby contributing to more robust framework evaluations.

### 7.2.3 Thematic analysis

A thematic analysis was used to discover common patterns and weaknesses in cases of ghost worker fraud. This qualitative analysis approach is distinguished by its flexibility and rigour, allowing researchers to find, analyze, and report themes in qualitative data [73]. Thematic analysis is particularly useful in exploratory research because it allows for the integration of several data sources and the emergence of themes that could inform theoretical frameworks [408].

Thematic analysis consists of several critical stages: familiarisation with the data, generation of initial codes, searching for themes, reviewing themes, defining and naming theses, and final producing the report [73]. Alyami et al. used theme analysis to assess the effectiveness of information security frameworks in preventing data breaches [25]. By using the qualitative analysis, general frameworks and information security frameworks were identified from the literature. The paper presents a framework for evaluating group behaviour in information security based on information security behavioural threshold analysis.

Similarly, Beardsmore and McSherry employed theme analysis to study how organizational culture affects the adoption of compliance frameworks in the healthcare sector [47]. Through qualitative interviews with healthcare workers, they discovered themes relating to change resistance and the need of leadership support. Qualitative interviews with healthcare professionals revealed themes concerning resistance to change and the necessity of leadership support. Their research demonstrates how thematic analysis can uncover fundamental cultural factors that affect the effective execution of compliance protocols.

Equally, Machen illustrated the application of thematic analysis in their examination of patient safety incidents within healthcare [236]. He identified significant themes that contributed to recurring safety issues by analysing qualitative data. The themed review approach provided better insight into the complexities and nuances of the system of safety, rather than just focusing on individual errors or policy non-compliance. This study underscores the significance of thematic analysis in recognising systemic weaknesses and informing the development of effective solutions. In the context of this evaluation, the thematic analysis made it possible to identify major vulnerabilities across the 8 fraud cases involving ghost workers. These vulnerabilities included problems such as inadequate data validation, insufficient oversight, and a lack of collaboration between agencies. These identified themes not only give a platform for analysing how the proposed decentralized validation framework could address these vulnerabilities, but they also reflect the systemic deficiencies that are present in the employment processes that are now in place.

#### Process and Validation of thematic analysis

The thematic analysis followed the principles outlined by V. Braun and Clarke and was conducted in several stages [73]:

1. Familiarisation: Reading and summarising all selected case documents to identify fraud methods, organisational context, and weaknesses.

2. Initial coding: Extracting codes such as “single point of failure”, “manual vali-

dation loophole", "collusion risk", and "lack of external oversight".

3. Theme development: Grouping codes into broader themes, including; centralisation risk, susceptibility to internal collusion, and ineffectiveness of reactive audits.

4. Mapping to framework: Assessing whether and how the DEIFP framework could mitigate these themes through features like decentralised validation, observer roles, and immutable logging.

**Validation of analysis**

Initial thematic coding and interpretation was shared and discussed with the research supervisor and presented to some Nigerian government employees. Meanwhile, constructive feedback was used to refine code definitions and ensure themes were not selectively framed to favour the proposed framework.

**Analytical techniques and why chosen:** Several qualitative analytical methods were used; thematic analysis, which is to identify recurring patterns and systemic weaknesses across cases. Secondly, cross-case synthesis which is to compare and contrast how the DEIFP framework might perform in different organisational and geographical contexts. These methods are recommended in Design Science Research (DSR) evaluation, particularly when evaluating an artefact (here, the DEIFP framework) against known real-world problems rather than a functional prototype.

**Bias Reflection:** Recognising the risk of bias is important for transparency. First, selection bias, the well-documented, high-profile cases were more likely to be included, potentially overestimating the framework's fit for all contexts. Secondly, researcher bias, as the designer of the DEIFP framework, there is a risk of interpreting cases to support its validity. The mitigation to curtail such baises includes engaging supervisory review and feedback during theme development. Also, clearly documenting cases where the framework may be less effective.

**Framework limitations:** Some of the perceived limitations include;

1. Potentially less effective in environments with poor digital infrastructure.
2. Vulnerable to politically motivated manipulation of validators.
3. Assumes minimum institutional willingness to participate in decentralised validation.

In summary, by detailing the search strategy, inclusion criteria, period focus, thematic analysis process, and acknowledging biases, this section strengthens the rigour and transparency of the case study evaluation. It demonstrates that the DEIFP framework was analyzed not only against favorable examples but also critically examined for weaknesses and limitations.

### 7.2.4 Framework evaluation

The effectiveness of the framework was evaluated through a methodical comparison of the key components of the proposed DEIFP framework with the vulnerabilities and weaknesses that were discovered in every case of ghost worker fraud. The use of this comparison method not only makes it easier to gain a more in-depth comprehension of the manner in which the framework might solve particular problems, but it also indicates the framework's potential effectiveness in preventing fraudulent acts of similar kind in the future.

The strategy used in this assessment fits with the research carried out by Joe and Kankpang, who used a case study approach to evaluate the effectiveness of fraud risk reduction strategies in Nigerian public service organizations [194]. Their research emphasized the need of a rigorous evaluation framework that enables the identification of gaps in existing processes. Using a similar framework evaluation methodology, this study seeks to provide actionable insights into how the proposed decentralized validation framework might improve the integrity of employment processes.

Additionally, Rashid et al. conducted a comparative analysis of several governance frameworks in their study on corporate fraud prevention [326]. They examined the efficiency of these frameworks by examining literature about corporate fraud as well as financial crime from 2003 to 2018. Their findings suggest that the internal control

system is the most effective strategy to prevent and identify corporate fraud which is the component of good governance. The use of this approach emphasizes the importance of comparing the components of the proposed framework to the vulnerabilities that have already been identified in order to ensure an effective evaluation.

More so, Blancaflor et al. utilized a comparative method to examine cybersecurity frameworks utilized by industries in the Philippines [63]. The purpose of this comparison was to provide a recommendation for organizations in adopting the framework that is the most suitable for the prevention and mitigation of cyber threats. The authors conducted a systematic evaluation of the existing cybersecurity framework literature and other documents. Through the utilization of case studies, they were able to demonstrate that implementing of a cybersecurity framework is necessary for the reduction of risks and the maintenance of business continuity.

Furthermore, they were able to offer a framework and a common language for risk mitigation in situations where organizations are confronted with cyber risks and threats. This work is a helpful resource for demonstrating how comparative evaluations could lead to practical recommendations for improving security measures. In the context of this study, the framework evaluation was organized around several key components, such as decentralized data sharing, strong verification process, stakeholder collaboration, access Control and security, and feedback mechanisms. Each component was evaluated in light of the specific vulnerabilities discovered in the investigated ghost worker fraud cases.

## 7.3 Crime script analysis and its relevance to ghost worker fraud

Crime script analysis (CSA) is a useful method for analyzing and combating various types of fraud, particularly those perpetrated on the internet. Complex frauds such as the Madoff Investment Scheme have been examined using CSA, which has been used to pinpoint important actions and chances for prevention [165]. Junger et al. have conducted research that has used CSA to analyze frauds against businesses, including

phantom invoices and CEO-fraud [198]. This research has revealed both online and offline methods.

Similar fraud scripts use victim communication, enabler recruiting, and money mules, suggesting preventative methods [219]. CSA has also been used to investigate illegal, unreported, and unregulated (IUU) fishing and seafood fraud, identifying regulatory issues and making recommendations for more effective preventative measures [311]. These studies show how flexible CSA is in comprehending several kinds of fraud and pointing up areas of intervention to stop criminal behaviour. For this research, crime script analysis is a valuable method for understanding the dynamics of ghost worker fraud in Nigeria's public sector payroll system.

Understanding how this fraud unfolds step-by-step will provide crucial insights into how it could be prevented and where the DEIFP Framework could intervene effectively. By using a crime script analysis approach, we can break down the process of ghost worker fraud into distinct stages, identify the vulnerabilities at each step, and determine how the proposed decentralized framework could address these weaknesses.

### 7.3.1 Applying crime script analysis to ghost worker fraud

A typical crime script for ghost worker fraud consists of several key steps. Each of these steps represents a crucial action taken by the fraudster to manipulate the system. The process is not linear, and multiple actors, both internal and external, may play a role at different stages of the fraud. Below is an outline of the crime script for ghost worker fraud and an analysis of how the DEIFP Framework could address each stage:

**Step 1: Identifying opportunities in the system**

- Action: The fraudster identifies a weakness or vulnerability in the payroll system, such as lack of cross-agency verification or weak access control mechanisms.
- Vulnerabilities Identified: Weak monitoring, insufficient real-time data validation, lack of stakeholder collaboration.
- DEIFP Intervention: By decentralizing the payroll data and involving multiple

stakeholders (e.g., ministries, regulatory bodies), the system becomes less prone to manipulation by a single actor. Also, the introduction of strong verification process by independent validators ensures that any discrepancies are immediately flagged, reducing opportunities for fraud.

**Step 2: Manipulating the payroll system**

- Action: The fraudster adds ghost workers to the payroll system or alters existing records. This can include creating fake identities or reactivating former employees who no longer work for the government.
- Vulnerabilities Identified: Weak internal controls, poor data validation practices.
- DEIFP Intervention: The DEIFP framework's real-time validation mechanism ensures that any addition or modification of payroll records is instantly checked against existing records. Moreover, applying the Role-Based Access Control (RBAC), the DEIFP framework would restrict access to sensitive payroll data to authorized personnel only, ensuring that unauthorized changes are flagged immediately.

**Step 3: Approving fraudulent entries**

- Action: The fraudulent records are processed and approved within the payroll system, and ghost workers are officially added to the payroll.
- Vulnerabilities Identified: Lack of cross-agency validation, absence of monitoring.
- DEIFP Intervention: Utilizing the Stakeholder Collaboration, by involving multiple independent validators, such as the Ministry of Finance, the EFCC, and the police, the DEIFP framework prevents fraudulent entries from being processed without adequate review. In addition, decentralized verification ensures that no single entity could approve fraudulent entries, and all changes are subjected to scrutiny from multiple independent bodies.

**Step 4: Processing payments**

- Action: Payments are processed for ghost workers, and fraudulent funds are diverted to the fraudsters or their collaborators.
- Vulnerabilities Identified: Weak oversight, no real-time monitoring.
- DEIFP Intervention: Using the blockchain-based Audit Trail, the DEIFP framework creates an immutable record of all payroll transactions. The blockchain ledger ensures that any fraudulent payments can be traced back to the source, making it difficult for fraudsters to hide their actions. Also, feedback mechanism could allow employees or stakeholders to report suspicious payroll entries, enabling quick intervention to prevent further fraudulent payments.

**Step 5: Concealment of fraudulent activity**

- Action: Fraudsters may attempt to conceal their fraudulent actions by deleting records or transferring funds quickly to prevent detection.
- Vulnerabilities Identified: Lack of real-time auditing, no feedback mechanism.
- DEIFP Intervention: The Immutable Ledger ensures that activities to the payroll data are recorded in the blockchain, making it impossible for fraudsters to alter or delete records without detection. Also, continuous audit and monitoring of the blockchain ledger and feedback systems ensures that any irregularities are detected and flagged immediately.

### 7.3.2 How the DEIFP framework interrupts the fraud process

By understanding each stage of ghost worker fraud, we could observe how the DEIFP Framework effectively intervenes at critical points to prevent the fraud from occurring or going undetected. The key strengths of the DEIFP framework—such as decentralized data sharing, strong verification process, stakeholder collaboration, and feedback mechanisms—address each stage of the fraud process. Here's how the DEIFP framework disrupts the fraud script at each stage:

1. Stage 1 (Identifying Opportunities): The introduction of cross-agency collaboration and strong verification process significantly reduces the opportunities for fraudsters to identify weaknesses in the system.
2. Stage 2 (Manipulating the System): The DEIFP framework's strong verification process and role-based access control prevent fraudsters from manipulating payroll records without detection.
3. Stage 3 (Approving Fraudulent Entries): Decentralizing the verification process and introducing independent validators ensures that no single entity has the power to approve fraudulent entries without oversight.
4. Stage 4 (Processing Payments): Blockchain technology guarantees transparency and traceability, making it impossible for fraudulent payments to go unnoticed.
5. Stage 5 (Concealment): The immutable ledger and audit trails ensure that fraudsters cannot hide their actions, and the feedback mechanism allows for early detection and reporting.

### 7.3.3 Benefits of crime script analysis in understanding ghost worker fraud

Crime script analysis allows us to gain a detailed, step-by-step understanding of how ghost worker fraud operates and where it could be prevented. It is an essential tool for identifying both the immediate actions of fraudsters and the systemic weaknesses within the payroll system that allow fraud to flourish. By mapping out the crime process, crime script analysis helps to:

1. Identify Weaknesses: It clearly identifies the specific weaknesses in the payroll system at each stage of the fraud process.
2. Target Interventions: It enables targeted interventions at each step to disrupt the fraud process.
3. Design Effective Frameworks: It helps design frameworks address fraud at multiple levels, from detection to prevention.

**Conclusion** Crime script analysis would provide a systematic and in-depth approach to understanding how ghost worker fraud operates within Nigeria's public sector payroll system. By breaking the fraud process into distinct stages, I was able to identify where the fraud occurs and how it could be prevented. The DEIFP Framework is designed to disrupt each step of this process, offering a comprehensive solution to combat ghost worker fraud. This chapter has demonstrated the value of crime script analysis in informing the development of effective anti-fraud frameworks and policies.

## 7.4 Cases analysed

The aim of this section is to present a thorough evaluation of how the proposed framework could effectively address the systemic vulnerabilities that have allowed ghost worker fraud to continue to grow.

### 7.4.1 Analysis of three ghost worker fraud cases

Three cases stand out due to their scale and impact: the Anthony Ogar and Others (August 2020) case, defrauding the Nigerian government of approximately ₦140 million (74 000 GBP) [396], the Dairo Samson (2017) case defrauding the government of around ₦11.3 million (6 000 GBP) [125] [395], and the ICPC's uncovering of 22,074 suspicious workers in Ministries, Departments, and Agencies (MDAs) in 2024 defrauding the governement the the sum of ₦34.8 billion (approximately 184 000 000 million GBP) [283]. These cases illustrate how weaknesses in access control, lack of strong verification process, inadequate cross-agency collaboration, and insufficient internal controls contribute to the persistence of ghost worker fraud. In each case, perpetrators were able to manipulate payroll data, creating fictitious employees and siphoning off public funds intended for legitimate government workers.

**Vulnerabilities identified:** Across all three cases, several vulnerabilities were identified in the existing payroll systems, including:

- Weak Access Control and Oversight: The fraudsters exploited weak access control

mechanisms, allowing unauthorized individuals to manipulate payroll data.

- Lack of strong verification process: In the absence of strong verification mechanism, fraudulent entries were not flagged immediately, allowing ghost workers to remain undetected for extended periods.
- Absence of Cross-Agency Verification: Limited collaboration between various government agencies allowed fraudulent data to pass unchecked, with insufficient mechanisms to cross-verify employment records.
- Inadequate Internal Controls: Many of the fraudulent activities persisted due to the lack of robust internal checks and auditing procedures.

**How the DEIFP framework could have prevented these frauds:** The DEIFP framework, with its blockchain-based decentralized data sharing and strong verification process, could have significantly reduced the risk of fraud in these cases:

- Decentralized Data Sharing: By involving multiple independent stakeholders, the DEIFP framework would ensures that no single entity has sole control over payroll data, reducing opportunities for manipulation.
- Strong verification process: The DEIFP framework's strong verification mechanism would have immediately flagged inconsistencies in the payroll, preventing the insertion of ghost workers into the system.
- Stakeholder Collaboration: A decentralized approach would have facilitated greater collaboration between various agencies, ensuring that employment records were cross-checked and validated from multiple sources, reducing the chances of fraud slipping through.
- Access Control and Security: The DEIFP framework's role-based access control (RBAC) system would have restricted unauthorized individuals from making changes to payroll records, ensuring that only authorized personnel had the ability to approve changes.

- Feedback Mechanism: The integrated feedback system would have allowed whistleblowers or other employees to report discrepancies in the payroll records, enabling early detection of fraudulent activities.

**Conclusion** The ghost worker fraud cases analyzed here highlight the critical flaws in Nigeria's existing payroll management systems, including weak internal controls, poor cross-agency verification, and inadequate access restrictions. By decentralizing payroll data verification, ensuring real-time validation, and fostering inter-agency collaboration, the DEIFP framework would offer the solution to address these weaknesses. Its features, such as blockchain technology and strong verification process, would provide a transparent, tamper-resistant, and secure framework for preventing ghost worker fraud and safeguarding public funds in Nigeria's public sector.

### 7.4.2 Analysis of Dr. Mzalendo Kibunja payroll and employment fraud analysis

Dr. Mzalendo Kibunja and his accomplices defrauded the National Museums of Kenya by creating and paying ghost workers. Dr. Kibunja, NMK Director General, and many collaborators embezzled Kes 449 392 075 (approximately 2 900 000 million GBP) by paying salary and gratuity to non-existent employees between January 2016 and February 2022. This fraud involved manipulating the payroll system to steal large amounts of money from the institution.

Several officials and a private individual committed the fraud. Oliver Okinyi Rabuor, Payroll ICT Officer; Wycliffe Odhiambo Ongata, Payroll Accountant; and Oscar Mwaura, a private individual implicated in the scam, were the accused. Stanvas Ongalo Opija, the Acting Director General during the fraud, failed to follow public finance management standards and contributed to the illegal disbursements. Investigations into payroll system anomalies found 105 ghost workers who were paid Kes 491 million over six years. These ghost workers were falsely added to the payroll as NM6s, a position that was part of a three-year renewable contract. Payments were made to nonexistent or former employees, and embezzled cash were laundered through bank accounts, including

M-Pesa accounts, making traceability difficult [122].

**Vulnerabilities identified:** Several flaws were discovered during the inquiry, which allowed the scam to continue for several years. Some weaknesses are:

- Insufficient Payroll Oversight: The main issue was improper payroll system manipulation without proper verification. Officials with payroll system access could create fake workers and make payments to them.
- Weak Internal Controls: Inadequate internal controls and auditing made large-scale embezzlement go undetected. The discovery of 105 ghost workers in NMK's 1,200-person workforce suggests payroll data oversight was lacking.
- Insufficient Financial Regulation Compliance: Stanvas Ongalo Opija, Acting Director General, failed to comply with Public Finance Management Regulations (2015), particularly Regulation 121, leading to ongoing fraud. He failed to implement financial controls or examine suspicious payments, a major vulnerability.
- Collusion Among Employees: Multiple employees were involved in the theft, suggesting collaboration to steal monies undetected. Oscar Mwaura, a private individual, received and laundered monies through shell businesses.
- Ineffective Verification Systems: Employee data was not cross-checked or validated against external systems, allowing fraudulent employees to remain on the payroll for years.
- Document Forgery and Financial crime: Ghost workers and NMK officials fabricated fake loan documents, putting the institution at danger and implicating banks in the crime.

**How the DEIFP framework could have prevented this fraud:** Key components of the DEIFP Framework could have solved the National Museums of Kenya payroll fraud case.

- decentralized Data Sharing: The DEIFP Framework uses the decentralized data sharing feature to prevent single individuals or departments from manipulating payroll records. Independent agencies would have validate and verify all personnel data updates in real time, preventing fraud. For instance, the DEIFP Framework would have flagged 105 ghost workers during data validation, as independent agencies like the CBN and IPPIS would have cross-verified employee information in a shared, immutable ledger.

- Strong verification process: The DEIFP Framework validates new personnel data in real-time. This would have immediately identified job status problems, preventing ghost workers from being added to the payroll. The system would have detected inconsistencies in identification or job status if Wycliffe Odhiambo Ongata had added ghost workers to the payroll during the probe, stopping illicit payments.

- Stakeholder Collaboration: Blockchain enabled decentralized verification and validation of personnel records by numerous agencies. This collaborative validation technique prevents data manipulation without notice, lowering fraud risk. For instance, the framework would have prevented Wycliffe Ongata, Oliver Okinyi Rabuor, and others from independently altering payroll data without alerts from validators and financial regulators, and law enforcement like the police and EFCC.

- Access Control and Security: Blockchain-based RBAC restricts the access and modification of employee records to authorized workers. This would have prevented unauthorized payroll data changes and restricted access to authorized users. For instance, the DEIFP framework restricted payroll adjustments to authorized people with certain duties, such as HR workers or auditors. Automatic alerts for unauthorized changes provided an audit trail to track fraud.

- Feedback Mechanism: The DEIFP Framework enables anonymous reporting of questionable activity by employees and stakeholders. This proactive reporting system would have detected ghost workers and fraud earlier. A whistleblower at the National Museums of Kenya may have reported suspect payroll entries

using the feedback system, leading to an urgent investigation and averting future corruption.

**Conclusion** The Dr. Mzalendo Kibunja case shows systemic problems such insufficient internal controls, inadequate employment record verification, and trusted personnel manipulating payroll data. These weaknesses let ghost worker fraud to continue for years, embezzling approximately Kes 491 million. The DEIFP Framework would have decentralized employment verification, enabled real-time validation, and improved stakeholder engagement. The DEIFP Framework might have used its features to manage employee data and reduce ghost worker fraud in the National Museums of Kenya and other public sector institutions. A system with decentralized data sharing, strong verification process, access restriction, and an effective feedback mechanism may have prevented this instance, saving millions of public monies and improving public sector employment processes.

### 7.4.3 Fraudsters convicted in Leicestershire (2020) for ghost worker fraud

In 2020, a case of ghost worker fraud was reported in Leicestershire, where a group of fraudsters was found guilty of arranging a scam that defrauded a cancer charity and the local council of thousands of pounds. The fraudsters were able to syphon off funds that were intended for legitimate employees by creating fake employee records [46]. Not only did this case result in financial losses for the organization, but it also brought to light severe vulnerabilities within the payroll management systems that allowed for such fraudulent activities to take place without being discovered. This entails a systemic failure to execute proper verification mechanisms. This failure allowed the fraudsters to manipulate the payroll without generating suspicion. The absence of rigorous control procedures and extensive background checks on employees, both of which are necessary components of any functioning payroll management system, made it easier for the fraudulent plan to be carried out. Because of this, the deficiencies of the payroll system were brought to light, highlighting the urgent requirement for stronger

security measures to protect against ghost workers fraud.

**Vulnerabilities identified:** Some of the vulnerabilities identified include:

- Lack of Thorough Background Checks on Employees: The current systems failed to perform thorough checks on employee records, allowing false entries to be made and authorized without verification. This lack of verification considerably increased the chance of fraudulent activity being undetected.
- Weak Oversight by Financial Management Entities: Inadequate oversight procedures in the financial management systems prevented them from spotting irregularities in payroll data that would point to fraud. As a result of this lack of vigilance, an environment where fraud could flourish was established.

**How the DEIFP framework could have prevented this fraud:** The proposed DEIFP framework could address the weaknesses revealed in the Leicestershire fraud case by providing specific solutions to improve payroll process integrity and reduce the risks associated with ghost worker fraud. In the context of this particular case, the following major components of the framework are particularly essential:

- Decentralized Data Sharing: The framework would enable real-time access to personnel records by facilitating secure data sharing across relevant agencies, such as the validating peers as well as the non-validating peers. This would be accomplished through the framework's decentralized data sharing. As a result of this transparency, it would be significantly more challenging for fraudulent individuals to generate fake personnel records without being discovered. For instance, if one had access to the decentralized ledger that was shared with other validating agencies (such as IPPIS and CBN), then anomalies in employee records might have been found in time.
- Strong verification process: The incorporation of strong verification mechanism into the framework would make it possible to validate newly added employee entries against the records that are already in place. In the situation involving

Leicestershire, such verification may have alerted authorities to the fact that fake personnel records were being created at the point of entry, which would have permitted them to initiate investigations immediately.

- Stakeholders Collaboration: The framework promotes collaboration among a variety of governmental and financial bodies, making it possible for these entities to work together to validate new employee records. It is absolutely necessary to work together in order to ensure that the payroll and employment system continues to function properly. In this instance, the fraud might have been discovered sooner and large financial losses might have been avoided if stakeholders had been involved in the verification process.

- Access Control and Security: The framework would ensure that only authorized workers are able to make changes to employee information by implementing stringent access restrictions. In the context of the Leicestershire case, these precautions could have limited the capacity of unauthorized individuals to create fake employee records, hence lowering the likelihood of fraudulent activity occurring.

- Feedback Mechanisms: The establishment of feedback channels via which employees and other stakeholders can report suspicious activity would improve the detection of abnormalities. Employees would have been able to express concerns about anomalies in payroll entries or employment process if such systems had been in place during the Leicestershire fraud case, allowing a faster response to fraudulent activity.

**Conclusion** The Leicestershire fraud case is an example of the weaknesses that might exist within payroll and employment process. It is possible for organizations in the public sector to improve their fraud prevention procedures, protect public funds, and guarantee that resources are given to legitimate personnel if they identify and correct these flaws through a decentralized validation framework. The DEIFP framework places focus on inter-agency collaboration, strong verification process, and stringent control as one of the most important factors in preventing future cases of ghost workers fraud

and, as a result, increasing the general integrity of employment processes.

### 7.4.4 Alisha Richardson case (2023)

In the year 2023, Alisha Richardson, who had previously worked at a nursing home in the Chicago region, was indicted on seven charges of wire fraud. She was accused of arranging a scam involving ghost employees that resulted in her company losing more than one hundred thousand dollars. Richardson fabricated personnel records to provide payments for people who were never really employed at the company, according to the indictment. To be more specific, she fabricated documentation in order to give the impression that these individuals were working as Certified Nursing Assistants and clocking in fictitious hours in order to make the process of payroll processing easier. Through the use of this fraudulent activity, she was able to obtain pay cheques for these fictitious employees. These pay cheques were either cashed by the individuals involved or deposited into Richardson's own bank accounts through the use of forged endorsements.

An investigation was conducted by the Federal Bureau of Investigation (FBI) and the Office of Inspector General of the Department of Health and Human Services (HHS) (Office of Public Affairs — Former Nursing Home Worker Charged with Wire Fraud in [405]. This case demonstrates enormous weaknesses in payroll and personnel verification systems within organizations, particularly in industries such as healthcare where trust and accountability are of the utmost importance. Not only did the fraudulent acts cause the nursing home to suffer significant financial losses, but they also diverted vital resources away from healthcare services that were intended to be provided to people who were in need. This investigation highlighted the seriousness of the fraud and the necessity of working together to confront criminal actions of this nature.

**Vulnerabilities identified:** The vulnerabilities identified are as follows:

- Inadequate Employee Verification Processes: There is a lack of effective verification methods inside the payroll and employment process of the nursing home, which is indicated by the fact that Richardson is able to generate false employee

records without being discovered. Because of this breach, fraudulent entries were able to pass through without being scrutinised, which allowed the ghost worker scheme to thrive.

- Weak Oversight and Accountability: Due to the lack of effective internal controls and oversight, the nursing home was unable to appropriately monitor payroll inputs, new staff or authenticate staff hours. Richardson was able to commit fraud over a prolonged period of time because there was a lack of accountability in the situation.

**How the DEIFP framework could have prevented this fraud:** The proposed DEIFP framework is well-suited to addressing the vulnerabilities identified in the Alisha Richardson case, as it includes measures to improve employee process payroll integrity and avoid similar fraud schemes. The following are important aspects of the framework that are relevant to this particular instance:

- Decentralized Data Sharing: The implementation of a decentralized system for sharing of employee data among key stakeholders, such as regulatory organizations and entities responsible for financial oversight, would make it possible to verify employee records in real time. In the case of Richardson, if there had been a decentralized database that was accessible to all validating agencies, it is quite likely that discrepancies in employment records would have been found early, so preventing the fraudulent conduct from becoming more widespread.

- Strong verification process: The framework's emphasis on strong verification process would make it possible to conduct immediate checks of information entered by employees against previously established records. The nursing home would have been able to initiate an instant inquiry into the discrepancies if it had utilized such a system.

- Stakeholder Collaboration: It is imperative to foster collaboration among relevant agencies of government in order to ensure the supervision of employee records and employment process. In this sense, improved cooperation may have enabled

regular audits and cross-checks of payroll entries and employment process, hence raising the possibility of early identification of fraudulent behaviour.

- Access Control and Security: Strict access limits could guarantee that payroll records and employment process may be modified only by authorized staff members. Given Richardson's situation, more robust access restrictions could have limited the ability to generate and alter ghost employee records free from supervision, therefore lowering the internal fraud risk.

- Feedback Mechanisms: Establishing feedback mechanisms for staff members and other stakeholders to report abnormalities in payroll entries or express concerns about suspected activity could help to improve the fraud detection. If such systems had been in place, members could have found discrepancies in employment data, which would have resulted in earlier intervention and fraud prevention.

**Conclusion** The Alisha Richardson case shows the weaknesses in payroll systems and lack of integrity in employment process. The systematic flaws found in this situation could be reasonably fixed by using the proposed decentralized validation framework. The framework's objective is to increase the overall integrity of employment processes and protect public funds, particularly in sensitive sectors like healthcare, by enhancing data sharing, strong verification process, and robust oversight mechanisms.

### 7.4.5 Fort Myers airport contractor case (2020)

A Fort Myers airport contractor was found guilty in 2020 of engaging in a ghost worker scheme, thereby defrauding the airport of around $900 000. The contractor forged payroll documents to increase the count of employees, hence misallocating monies intended for legitimate personnel. The contractor fabricated false personnel records rather than hiring real workers, which allowed them to keep the money that would have gone to the real workforce. An investigation uncovered discrepancies in the payroll system, and the contractor was charged for their involvement in the scheme [248]. The case draws attention to important flaws in the supervision and validation of contractor payroll entries.

Lack of transparency in the contractor management procedure and inadequate control of contractor-submitted payroll information facilitated the fraudulent behaviour. The contractor was thus able to control the payroll system for a long period, syphoning off money meant for reasonable uses.

**Vulnerabilities identified:** The vulnerabilities are as follows:

- Inadequate Monitoring of Contractor Payroll Submissions: The absence of careful examination of contractor payroll entries let the fraud to go unnoticed for a long amount of time. Lack of a good monitoring mechanism allowed the contractor to inflate payroll records and pocket money.
- Lack of Transparency in Contractor Management: The lack of explicit procedures for confirming the validity of new employees helped to explain the simplicity of the fraud committed. The lack of transparency made it challenging for the airport officials to efficiently monitor and check payroll entries.

**How the DEIFP framework could have prevented this fraud:** The proposed distributed validation framework is could be fit to solve the vulnerabilities found in the Fort Myers Airport Contractor issue. The main element of the framework are meant to improve payroll verification procedures, this element presents particular alternatives that might have stopped the scam and protected the scan from happening.

- Decentralized Data Sharing: One of the most important characteristics of the proposed framework is distributed data sharing, which helps to securely exchange employee data across appropriate parties. With real-time validation of employment process, Fort Myers Airport could have been cross-checked and validated all new staff, therefore ensuring the legitimacy of those records. This would have stopped the contractor from turning in ghost workers in the system.
- Strong verification process: The framework comprises strong verification mechanisms, which would guarantee that every employee is validated before payroll

detail is submitted. In the Fort Myers case, the system would have not recognized because they were not properly checked and validated during the hiring process. Automated checks might have promptly found the bogus claims by cross-referencing the entered records with actual employee data.

- Stakeholder Collaboration: The proposed framework enforced collaboration among government agencies, and ensure that employment record is accurate and up-to-date. Regarding the Fort Myers Airport, cooperation between the agencies and other peers such as EFCC and the police could have helped to enable routine audits and the employment verification. This cooperation would have added another level of assessment, which would have made it more difficult for the contractor to commit fraud undetectable.

- Access Control and Security: The framework stresses the need of access management to sensitive employment and payroll data. The system helps stop fraudulent activity by people in positions of power by restricting access to just authorized workers. In this situation, the framework would have allowed only authorized staff members of the airport and supervising authorities to change or approve employment records, therefore lowering the possibility of contractor manipulation.

**Conclusion** The Fort Myers Airport Contractor case emphasizes the crucial need of strong employment verification and monitoring procedures. The proposed decentralized validation approach could address the weaknesses identified in this case, such as inadequate monitoring of contractor employment and payroll submissions and a lack of transparency in contractor management. The framework proposes solution for preventing similar fraudulent acts and protecting public monies by incorporating elements such as strong verification mechanism, decentralized data sharing, stakeholder engagement, and strengthened access controls.

### 7.4.6 Analysis of the Vanguard Article on Ghost Workers Abroad (June 2024)

The Head of the Civil Service of the Federation, Dr. Folasade Yemi-Esan, revealed in June 2024 a successful crackdown on ghost workers, public servants paid while residing abroad or not working at all. This was part of the continuous attempt of the Nigerian government to eradicate public sector fraud, especially in the payroll and employment system. The exercise revealed that numerous people were still paid while living abroad and took advantage of weaknesses in the verification system. Dr. Yemi-Esan said that revealing this fraudulent behaviour had been greatly aided by the IPPIS.

According to the government's verifying process, some governmental personnel living overseas were nonetheless paid without doing their assigned tasks in Nigeria. These workers were obviously involved in fraudulent behaviour since they had neglected to take part in the physical verification process. The civil officers engaged in the fraud were told to resign, and an investigation into their actions was launched. Dr. Yemi-Esan observed that these fraudulent persons were frequently absent from the verification process, emphasizing the limits of depending entirely on IPPIS for employment verification [126].

**Vulnerabilities identified:** This case revealed several weaknesses that let ghost workers stay on the pay despite being absent or unfit:

- Inadequate means of validation: The main problem was depending just on a single verification system (IPPIS) without regular actual presence of staff. This let unqualified workers or those stationed overseas stay on the payroll unnoticed for a long time.

- Inadequate Follow-Up Procedures: After employees enrolled in the IPPIS system, not enough was done to verify their eligibility going forward, especially if they were assigned overseas or had non-governmental jobs.

- Limited Use of External Verification: Fraudulent employees were able to go unnoticed since there was no integrated system in place to cross-check employee status

with external databases overseas.

- Lack of Accountability and Transparency: Many of the fraudsters were permitted to keep receiving salary for a long time without any audits or checks. This underscores the absence of transparency in the payroll and employment management system.

**How the DEIFP framework could have prevented this fraud:** Many of these weaknesses may have been addressed by the DEIFP Framework:

- Decentralized Data Sharing: DEIFP framework enables collaboration among government agencies to assure employee validity. Cross-agency validation would have found disparities involving overseas based personnel. For instance, utilizing blockchain-based strong verification mrchanism, employees' overseas postings would have been cross-checked and verified, making sure only authentic ones are considered. In the event that there were any inconsistencies, they would have been reported promptly.

- Strong verification process: Employee data is regularly updated and cross-checked with other agencies to prevent fraudulent entries during and after recruitments. For instance, the system would have instantly identified the lack of verification or cross-referenced with outside records to indicate the problem if an employee working overseas kept receiving a pay without physical confirmation.

- Stakeholder Collaboration: The DEIFP Framework's decentralized structure would have enabled several stakeholders to independently verify personnel records, guaranteeing that any fraudulent activity was promptly identified.

- Access Control and Security: By limiting unauthorized individuals from altering payroll and employment records, blockchain's role-based access control (RBAC) would have stopped the unauthorized installation of ghost workers to the system. For instance, the smart contracts in the DEIFP system would have automatically blocked illegal employment access, therefore guaranteeing that only validated people may update job information.

**Conclusion** The crackdown on ghost workers abroad revealed major flaws in Nigeria's public sector payroll and employment system, particularly in the verification process. Fraudulent personnel were able to earn salary while stationed overseas since IPPIS was the only system used and there was no effective system in place to cross-check data with other agencies. The DEIFP Framework, which includes decentralized data sharing, strong verification process, stakeholder collaboration, and secure access control, would have significantly reduced these risks. The DEIFP Framework would use blockchain technology to provide more complete and transparent verification, preventing ghost workers from manipulating the system and securing public monies.

## 7.5 Summary of cases

A summary of the cases is provided in Table 7.1.

| S/N | Case/Link | Case Overview | Vulnerabilities Identified |
|---|---|---|---|
| 1 | Anthony Ogar and Others (August 2020) | A group of civil servants manipulated the IPPIS system, adding ghost workers to the payroll and defrauding the government of ₦140 million. The fraud was carried out by inserting fictitious employees into the system and siphoning off public funds. | Weak access control, lack of cross-agency verification, inadequate monitoring, lack of internal controls, failure to integrate third-party verification. |
| 2 | Dr. Mzalendo Kibunja Payroll Fraud (EACC - Kibunja Case) | Dr. Kibunja and collaborators embezzled ₦449 million by creating and paying salaries to ghost workers at the National Museums of Kenya (NMK). Over six years, they added 105 ghost workers to the payroll, laundering funds through M-Pesa accounts. | Insufficient payroll oversight, weak internal controls, collusion among employees, ineffective verification systems, document forgery. |
| 3 | Dairo Samson Fraud Case (2017) (EFCC - N11m Fraud) | Dairo Samson defrauded the Nigerian government of ₦11.3 million by adding ghost workers to multiple government agency payrolls and altering data. | Inadequate data validation, lack of strong verification process, lack of cross-agency verification. |

. . . continued

| S/N | Case/Link | Case Overview | Vulnerabilities Identified |
|---|---|---|---|
| 4 | Fraudsters Convicted in Leicestershire (2020) (Leicestershire Cancer Charity Scammers Jailed) | Fraudsters created fake employee records to siphon off funds intended for legitimate employees at a cancer charity and local council, leading to financial losses. | Lack of thorough background checks, weak oversight by financial management entities. |
| 5 | Alisha Richardson Case (2023) (FBI Wire Fraud Case) | Alisha Richardson, a nursing home employee, created fake employee records and falsely processed paychecks for non-existent workers, defrauding the company of over $100 000. | Inadequate employee verification, weak oversight, lack of accountability. |
| 6 | Fort Myers Airport Contractor Case (2020) (Fort Myers Airport Fraud) | A contractor for Fort Myers airport engaged in ghost worker fraud by submitting inflated payroll records, defrauding the airport of $900 000. | Inadequate monitoring of contractor payroll submissions, lack of transparency in contractor management. |
| 7 | Vanguard Article on Ghost Workers Abroad (June 2024) (Vanguard Ghost Worker Report) | The Nigerian government uncovered ghost workers on the payroll, including employees living abroad who were receiving salaries without performing any duties. | Inadequate means of validation, inadequate follow-up procedures, limited use of external verification, lack of accountability and transparency. |

. . . continued

| S/N | Case/Link | Case Overview | Vulnerabilities Identified |
|---|---|---|---|
| 8 | ICPC Uncovers 22,074 Suspicious Workers in MDAs (2024) (ICPC Suspicious Workers) | ICPC's review of the IPPIS revealed 22,074 suspicious employees across various Nigerian government MDAs. The fraud included ghost workers, duplicate payments, and discrepancies in employee records. | Data inconsistencies, payroll record manipulation, double payments, inadequate verification procedures, lack of cross-agency collaboration, absence of real-time monitoring, weak access control. |

Table 7.1: Summary of Ghost Worker Fraud Cases and DEIFP Framework Prevention

## 7.6 Conclusion

This chapter evaluates how well the DEIFP framework addresses employment fraud and ghost workers. By examining many well-publicized fraud cases, the chapter emphasizes systematic flaws in payroll and employment verification systems. Real-world fraud systems allow one to examine the consequences of poor access control, insufficient monitoring, and insufficient cross-agency verifying. The DEIFP system, which comprises decentralized data sharing, strong verification process, stakeholder engagement, access control and security, and a feedback mechanism, is being examined to reduce and prevent future fraud. The analysis shows how the DEIFP framework may improve employment processes and detect and prevent ghost worker fraud. In all the identified case studies, DEIPF would have removed vulnerabilities crucial to the execution of the fraud and so prevented it.

# Chapter 8

# Data analysis of the 2024 survey

This section analyzes the survey responses collected from government employees and blockchain experts regarding their perceptions of the IPPIS system and the proposed DEIFP in 2024. The analysis centred on two areas: First, the evaluation of the DEIFP framework, and second, analyzing the effectiveness and transparency of the IPPIS system in respect to ghost worker fraud and the employment process.

## 8.1 Survey design

Questionnaires are a common instrument in quantitative research for collecting data that provide numeric descriptions of a target population and trends [16]. To obtain reliable and valid data, the survey instrument in this study was carefully designed based on the literature and the contextual challenges of the Integrated Personnel and Payroll Information System (IPPIS) in Nigeria. In both the 2021 and 2024 studies, the survey instrument consisted of closed-ended questions to enhance ease of response and to increase response rates [110]. The survey items were derived after a comprehensive review of the literature on employment fraud and payroll systems, including works such as [39, 138, 180, 351, 440]. The objective was to ensure that the survey covered all relevant factors affecting the prevalence of ghost worker fraud, such as weaknesses in payroll management, governance gaps, and the perceived ineffectiveness of IPPIS. Key themes identified in the literature were then translated into specific, measurable survey questions. A Five-Point Likert Scale (Strongly Disagree = 1; Somewhat Disagree = 2; Neutral = 3; Somewhat Agree = 4; Strongly Agree = 5) was employed to capture the strength of respondents' perceptions. To strengthen construct validity, the survey questions were mapped directly to the study's six objectives as shown in Table 8.1.

This ensured that every question served a clear purpose in answering the overarching aims of the research.

Table 8.1: Mapping of Survey Questions to Research Objectives

| **Survey Question** | **Theme** | **Linked Objective(s)** |
|---|---|---|
| Q1: Status (employee/expert) | Classification of respondents | Supports all objectives by distinguishing perceptions across groups |
| Q2: Educational level | Demographics | Objective 1 – Perceptions shaped by background |
| Q3: Efficiency of IPPIS | Effectiveness of payroll system | Objective 1 – Understand employee perceptions |
| Q4: IPPIS provides transparency | Governance and accountability | Objective 1 – Perceptions of IPPIS effectiveness |
| Q5: IPPIS contributes to ghost worker fraud | Fraud drivers | Objective 1 – IPPIS link to fraud |
| Q6: Government monitoring mechanisms | Oversight | Objective 2 – Fraud frameworks (control mechanisms) |
| Q7: Corruption in payroll management | Systemic corruption | Objective 2 – Fraud theoretical analysis |
| Q8: Peer validation importance | Decentralised verification | Objective 3 – Developing blockchain framework |
| Q9: Independent validators (EFCC, judiciary) | Multi-stakeholder governance | Objective 4 – Defining stakeholder roles |
| Q10: Blockchain suitability for payroll | Applicability of blockchain | Objective 3 – Develop blockchain-based framework |
| Q11: Blockchain enhances transparency | Transparency via technology | Objective 3, Objective 6 – Framework development and evaluation |

Continued on next page

**Table 8.1 – continued from previous page**

| Survey Question | Theme | Linked Objective(s) |
|---|---|---|
| Q12: Blockchain improves security | Security mechanisms | Objective 3, Objective 6 – Framework robustness and evaluation |
| Q13: Blockchain improves efficiency | Performance improvement | Objective 3, Objective 6 – Framework robustness and evaluation |
| Q14: Blockchain adoption challenges | Barriers to adoption | Objective 6 – Effectiveness and recommendations |
| Q15: Blockchain increases employment integrity | Integrity outcomes | Objective 3, Objective 6 – Framework impact and evaluation |
| Q16: Stakeholder collaboration is necessary | Governance and collaboration | Objective 4 – Stakeholder roles |
| Q17: Blockchain reduces single point of failure | Decentralisation | Objective 3 – Blockchain framework justification |
| Q18: Feedback mechanism is important | Continuous improvement | Objective 4 – Stakeholder responsibilities |
| Q19: Trust in blockchain validators | Trusted nodes | Objective 3, Objective 4 – Security and governance of DEIFP |
| Q20: Blockchain reduces ghost worker fraud | Fraud mitigation | Objective 5, Objective 6 – Framework case study evaluation and survey assessment |
| Q21: Willingness to adopt blockchain in government | Adoption feasibility | Objective 6 – Practical adoption and assessment |

Continued on next page

**Table 8.1 – continued from previous page**

| Survey Question | Theme | Linked Objective(s) |
|---|---|---|
| Q22: Overall perception of DEIFP framework | Overall framework evaluation | Objective 5, Objective 6 – Case study analysis and survey evaluation |

By explicitly linking each survey item to the six research objectives, the survey design demonstrates internal coherence. For instance, questions Q3–Q7 primarily address Objective 1 and 2, capturing employee perceptions of IPPIS and connecting these insights to established fraud theories. Questions Q8–Q19 operationalise Objectives 3 and 4, focusing on the design, decentralisation, and governance of the proposed blockchain-based DEIFP framework. Finally, Q20–Q22 provide direct input into Objectives 5 and 6, offering both case-based and perception-based evaluations of the framework's effectiveness and adoption feasibility. This structured mapping ensures that the survey instrument directly supports the research's overarching goals.

### Recruitment of Participants

Participants were recruited through a combination of digital and direct outreach strategies. The two groups of participants are federal government employees in Nigeria who are currently working in ministries, departments, or agencies and are enrolled on the IPPIS platform. The second are the blockchain experts with demonstrable experience in blockchain development, implementation, or research. For government employees, survey links were distributed primarily through WhatsApp groups commonly used for departmental coordination and communication within ministries departments, and agencies. This method enabled rapid distribution across a wide pool of potential respondents. Additionally, direct phone calls were made to some government employees to encourage participation. For blockchain experts, recruitment was conducted by reaching out to professional networks, referrals, and targeted calls to developers, and researchers known to have expertise in blockchain systems. This dual strategy ensured representation from both the operational stakeholders of IPPIS and technical experts

in decentralised solutions.

### Participants' Briefing on DEIFP

To ensure that all participants could meaningfully respond to the survey, a structured briefing on the proposed DEIFP framework was provided prior to questionnaire completion. This briefing was included within the Participant Information Sheet (PIS) (see Appendix G), which stated the study's purpose and background. The PIS also contained a simplified description of the DEIFP framework, its purpose and the framework components, highlighting its validator and decentralized structure. By embedding the briefing directly in the PIS, participants were able to review and familiarise themselves with the framework before responding. This was particularly important for government employees who might have limited technical knowledge of blockchain.

### Replicability and Response Rate

In order to improve replicability, detailed recruitment records and participation rates were documented. Questionnaires were distributed and a total of 152 was obtained, out of which 144 were valid. Among these, 136 respondents identified as federal government employees and 8 as blockchain experts. The survey achieved adequate representation from both categories, although government employees were significantly more numerous, reflecting the public sector orientation of the study. The clear documentation of sampling, inclusion criteria, and briefing procedures enhances the study's replicability and provides transparency for future researchers wishing to evaluate similar interventions.

### Inclusion of Supporting Documentation

To strengthen transparency and replicability, the following documents are now included as appendices: the 2024 Ethics Application (see Appendix E), the 2024 Ethics Approval Email (see Appendix F), the 2024 Participant Information Sheet  Appendix G), and the Consent Form (see Appendix H).

## 8.2 Ethical consideration

The Department of Computer and Information Sciences approved the ethics application of 2024 survey with the application ID of 2764 (see Appendix F). Participants were told that their responses would be kept anonymous and used only for the purpose of this research. The ethical integrity of the research process was maintained to ensure that the results were credible, respectful and conducted in accordance with established research ethics.

## 8.3 Methodological approach of pilot testing

The pilot study involved a purposive sample of respondents drawn from government institutions and other researchers. Participants were selected based on they being employed and enrolled on the IPPIS and while some on their experience with the blockchain. The questionnaire was administered through the WhatsApp platform, while few were personally distributed to colleagues in the department who are employees of Nigerian government, and responses were collected anonymously to reduce social desirability bias. The pilot instrument included items grouped into thematic categories aligned with the study's conceptual framework, including, perceived effectiveness of IPPIS, trust in system integrity, likelihood of fraud reduction etc. Respondents were asked to rate each item using a 5-point Likert scale. In this study, the pilot test was conducted to evaluate the clarity, consistency, and reliability of a 25-item questionnaire designed for the exercise.

### 8.3.1 Reliability Analysis

This study used Cronbach's alpha reliability coefficient "$\alpha > 0.7$" to measure the survey questionnaire for internal reliability using SPSS. The idea is to determine internal consistency of scale, and how consistent people respond to the questions. The results are presented in 8.2. The pilot result in Table 8.2 shows that Cronbach's alpha efficiency of 0.711, which is an acceptable value because it is higher than the reference value of

Table 8.2: Reliability Statistics for Pilot Test

| **Statistic** | **Value** |
|---|---|
| Cronbach's Alpha | 0.711 |
| Number of Items | 25 |

0.7 [163]. The result suggests that the items are reasonably correlated and measure a coherent construct.

**Conclusion** Beyond overall reliability, item-level diagnostics were conducted to identify problematic items. Based on this, some items were reworded to improve clarity, three questions were removed entirely due to redundancy and low item-total correlation. Also, minor adjustments were made to the wording of technical terms to ensure accessibility across respondent groups. The pilot study provided strong evidence for the reliability and clarity of the instrument. The acceptable Cronbach's Alpha score, combined with item-level diagnostics and participant feedback, supports the instrument's readiness for full-scale deployment.

## 8.4 2024 Survey Confidence Interval Data Presentation and Analysis

Below is the presentation and analysis of the CIs of 2024 survey, including the table and the CI plot.

The summary Table 8.3 reveals varying degrees of confidence across survey items. For instance: Q21 had a high mean (4.60) and a narrow error ($\pm$0.40), suggesting strong consensus and high confidence that the sample reflects the population. In contrast, Q4 and Q6 exhibited wider intervals ($\pm$2.69 and $\pm$2.78 respectively), indicating more variability in responses and less certainty about population-level agreement. These results imply that while the proposed framework is broadly supported and perceived positively, opinions on the existing system are more divided, and thus less generalizable. The confidence intervals provide empirical support for the external validity of the study. Where intervals are narrow and centered around high means, we can reasonably infer

Table 8.3: Summary of Confidence Interval Statistics for Survey Questions

| **Question** | **Mean** | **Lower CI** | **Upper CI** | **Error (±)** |
|---|---|---|---|---|
| Q1 | 1.06 | 1.00 | 2.00 | 0.94 |
| Q2 | 4.21 | 3.00 | 5.00 | 1.06 |
| Q3 | 2.40 | 1.00 | 5.00 | 2.60 |
| Q4 | 2.31 | 1.00 | 5.00 | 2.69 |
| Q5 | 3.07 | 1.00 | 5.00 | 1.93 |
| Q6 | 2.22 | 1.00 | 5.00 | 2.78 |
| Q7 | 4.00 | 2.00 | 5.00 | 1.00 |
| Q8 | 3.94 | 3.00 | 5.00 | 1.06 |
| Q9 | 4.22 | 2.00 | 5.00 | 0.78 |
| Q10 | 4.01 | 2.00 | 5.00 | 0.99 |
| Q11 | 4.06 | 2.00 | 5.00 | 0.94 |
| Q12 | 4.08 | 2.00 | 5.00 | 0.92 |
| Q13 | 4.32 | 3.00 | 5.00 | 0.68 |
| Q14 | 4.07 | 2.00 | 5.00 | 0.93 |
| Q15 | 4.16 | 2.00 | 5.00 | 0.84 |
| Q16 | 4.34 | 3.00 | 5.00 | 0.66 |
| Q17 | 4.47 | 3.00 | 5.00 | 0.53 |
| Q18 | 4.42 | 3.00 | 5.00 | 0.58 |
| Q19 | 4.36 | 3.00 | 5.00 | 0.64 |
| Q20 | 4.47 | 3.00 | 5.00 | 0.53 |
| Q21 | 4.60 | 3.00 | 5.00 | 0.40 |
| Q22 | 4.55 | 3.00 | 5.00 | 0.45 |

that similar perceptions would be observed in the wider population. Conversely, wider intervals warrant caution in making broad claims.

## 8.5 Data presentation and analysis

The data collected were quantitative and were collected using the online Qualtrics survey tool [121]. There were 152 responses to the questionnaire from government employees and blockchain experts. The government employees (n = 136, 94.4%) identified as Federal Government Employees, while all blockchain experts (n = 8, 5.6%) identified

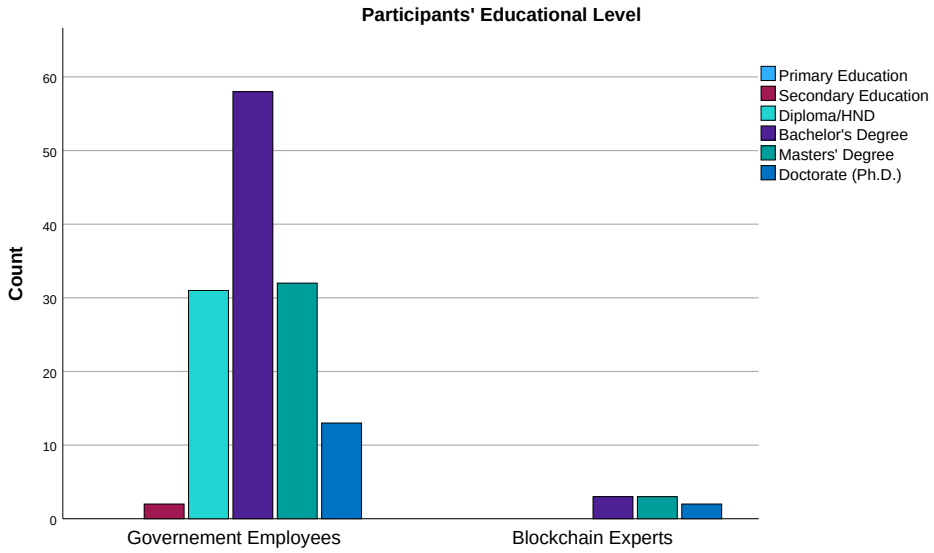


Figure 8.1: Participants' Educational Level

as Blockchain Experts. These are the two categories that segmented participants into distinct groups. Descriptive statistics were used to report the findings of the individual question. Each question sought the perceptions of blockchain experts and government employees regarding the efficiency of the IPPIS and the proposed DEIFP framework. Below are the tables and bar charts for the questions with their corresponding explanations. Table 8.4 and Figure 8.1 reveal distinct educational profiles between govern-

Table 8.4: Q2: What is your highest level of education?

| | Government Employees | | Blockchain Experts | | Total | |
|---|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count | % of Total |
| Secondary | 2 | 1.4% | 0 | 0.0% | 2 | 1.4% |
| Dip/HND | 31 | 21.5% | 0 | 0.0% | 31 | 21.5% |
| Bachelor's | 58 | 40.3% | 3 | 2.1% | 61 | 42.4% |
| Master's | 32 | 22.2% | 3 | 2.1% | 35 | 24.3% |
| Doc (PhD) | 13 | 9.0% | 2 | 1.4% | 15 | 10.4% |
| Total | 136 | 94.4% | 8 | 5.6% | 144 | 100.0% |

ment employees and blockchain experts. Among government employees (n = 136), the majority hold a Bachelor's degree (40.3%), followed by Master's degrees (22.2%) and

Diploma/HND qualifications (21.5%). A smaller proportion have attained Doctorate degrees (9.0%), while only 1.4% reported Secondary Education as their highest qualification. In contrast, blockchain experts (n = 8) show a more advanced academic profile: 62.5% hold postgraduate degrees (Master's or Ph.D.), and the remaining 37.5% possess Bachelor's degrees. None reported lower-level qualifications. This distribution suggests that blockchain experts tend to have higher academic attainment, likely reflecting the technical and research-oriented nature of their field. Government employees, while also well-educated, show a broader range of qualifications, consistent with the diversity of roles within public service. Though small size for experts makes comparison limited.

Table 8.5: Q3: How would you rate the efficiency of the IPPIS in managing employment records and payroll?

| | Government Employees | | Blockchain Experts | | Total | |
|---|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count | % of Total |
| Very inefficient | 35 | 24.3% | 3 | 2.1% | 38 | 26.4% |
| Inefficient | 60 | 41.7% | 0 | 0.0% | 60 | 41.7% |
| Neutral | 10 | 6.9% | 2 | 1.4% | 12 | 8.3% |
| Efficient | 17 | 11.8% | 2 | 1.4% | 19 | 13.2% |
| Very efficient | 14 | 9.7% | 1 | 0.7% | 15 | 10.4% |
| Total | 136 | 94.4% | 8 | 5.6% | 144 | 100.0% |

Table 8.5 and Figure 8.2 indicate that government employees overwhelmingly viewed IPPIS as ineffective, with 41.7% rating it "inefficient" and 24.3% "very inefficient," compared to just 21.5% reporting it as efficient. Blockchain experts were less negative, with 37.5% also judging it inefficient but an equal 37.5% expressing neutral or positive views. This divergence can be explained by the fact that employees directly experience the administrative shortcomings and frustrations of the system, while experts tend to evaluate it from a technical or conceptual standpoint, recognising potential operational merits despite its implementation flaws. Table 8.6 and Figure 8.3 presents respondents' views on the transparency of IPPIS in the employment process. Among government employees, a substantial majority (67.4%) expressed negative perceptions. Only 20.1% indicated agreement, while 6.9% remained neutral. In contrast, blockchain experts were less critical: although 37.5% strongly disagreed, half of the group (50%)

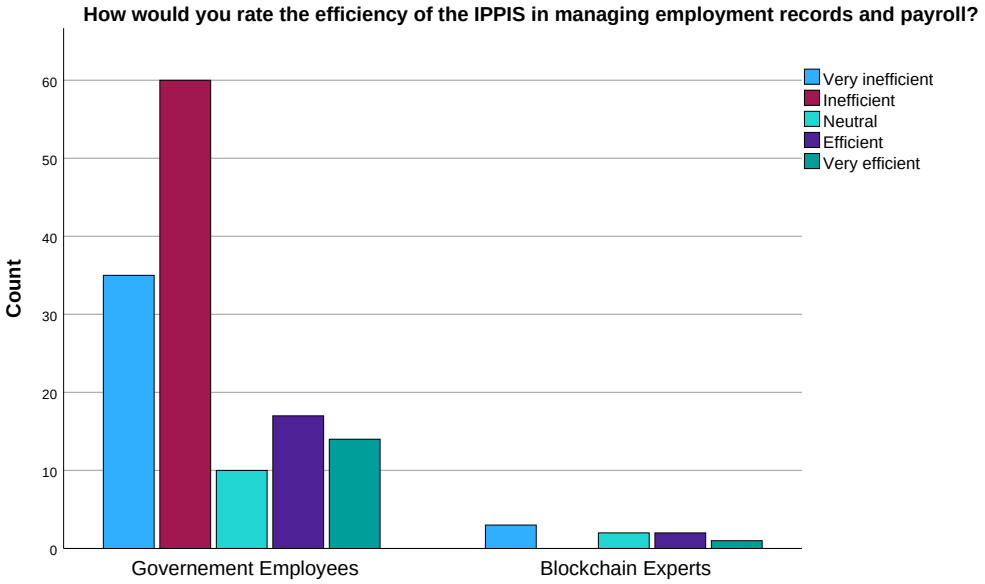


Figure 8.2: How would you rate the efficiency of the IPPIS in managing employment records and payroll?

Table 8.6: Q4: To what extent do you agree that IPPIS provides transparency in the employment process?

| | Government Employees | | Blockchain Experts | | Total | |
|---|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count | % of Total |
| Strongly disagree | 42 | 29.2% | 3 | 2.1% | 45 | 31.3% |
| Disagree | 55 | 38.2% | 0 | 0.0% | 55 | 38.2% |
| Neutral | 10 | 6.9% | 1 | 0.7% | 11 | 7.6% |
| Agree | 18 | 12.5% | 3 | 2.1% | 21 | 14.6% |
| Strongly agree | 11 | 7.6% | 1 | 0.7% | 12 | 8.3% |
| Total | 136 | 94.4% | 8 | 5.6% | 144 | 100.0% |

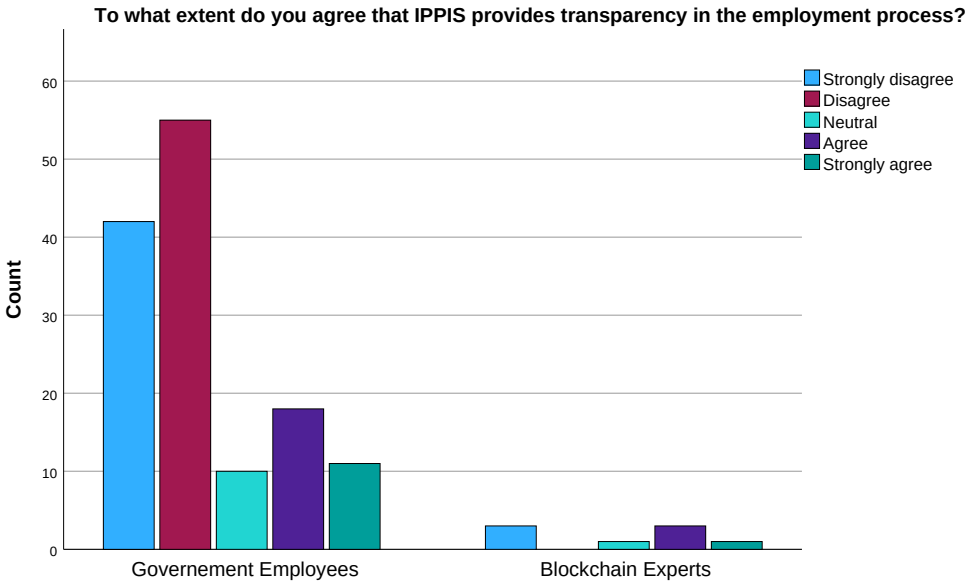


Figure 8.3: To what extent do you agree that IPPIS provides transparency in the employment process?

reported neutral or positive views. This divergence likely reflects differing perspectives, that is government employees engage with IPPIS operationally, while experts assess its conceptual design and potential. Looking at the information from Table 8.7 and Figure 8.4, both groups acknowledged the potential link between IPPIS and ghost worker fraud, though with varying degrees of conviction. Among government employees, 43% agreed or strongly agreed that IPPIS contributes to the issue, while 40.2% disagreed or

Table 8.7: Q5: To what extent do you agree that IPPIS contributes to the issue of ghost worker fraud?

| | Government Employees | | Blockchain Experts | | Total | |
|---|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count | % of Total |
| Strongly disagree | 30 | 20.8% | 0 | 0.0% | 30 | 20.8% |
| Disagree | 28 | 19.4% | 2 | 1.4% | 30 | 20.8% |
| Neutral | 16 | 11.1% | 3 | 2.1% | 19 | 13.2% |
| Agree | 30 | 20.8% | 0 | 0.0% | 30 | 20.8% |
| Strongly agree | 32 | 22.2% | 3 | 2.1% | 35 | 24.3% |
| Total | 136 | 94.4% | 8 | 5.6% | 144 | 100.0% |

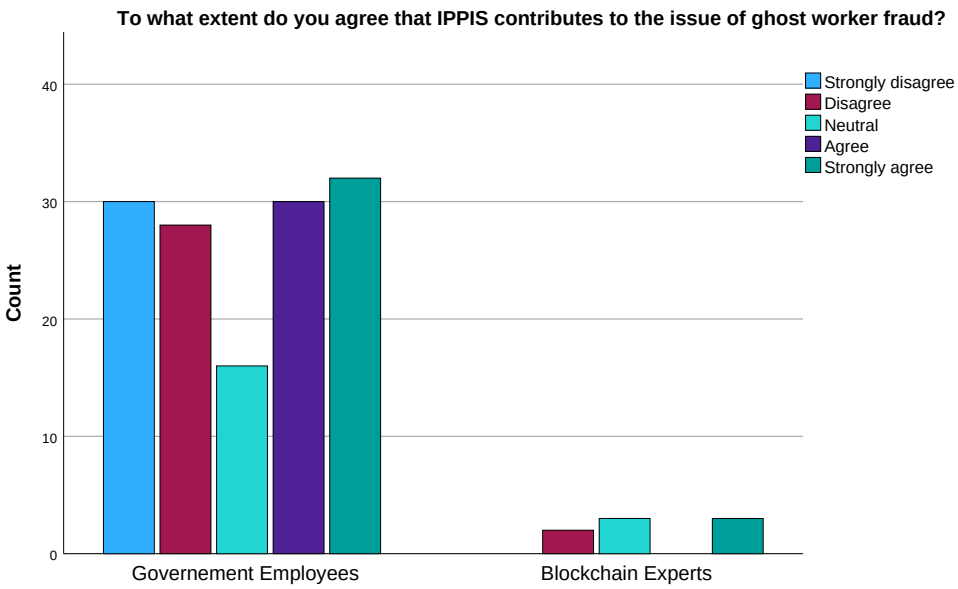


Figure 8.4: To what extent do you agree that IPPIS contributes to the issue of ghost worker fraud?

strongly disagreed. A smaller segment (11.1%) remained neutral. Blockchain experts showed a more critical stance, with 37.5% strongly agreeing and 25% remaining neutral. Both groups expressed concerns about the effectiveness of IPPIS in preventing

Table 8.8: Q6: How effective do you think IPPIS is in preventing ghost worker fraud?

| | Government Employees | | Blockchain Experts | | Total | |
|---|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count | % of Total |
| Very inefficient | 48 | 33.3% | 3 | 2.1% | 51 | 35.4% |
| Inefficient | 48 | 33.3% | 1 | 0.7% | 49 | 34.0% |
| Neutral | 13 | 9.0% | 1 | 0.7% | 14 | 9.7% |
| Efficient | 21 | 14.6% | 1 | 0.7% | 22 | 15.3% |
| Very efficient | 6 | 4.2% | 2 | 1.4% | 8 | 5.6% |
| Total | 136 | 94.4% | 8 | 5.6% | 144 | 100.0% |

ghost worker fraud, though with differing intensities as shown in Table 8.8 and Figure 8.5. Among government employees, 66.6% rated the system as either inefficient or very inefficient, while only 18.8% considered it efficient or very efficient. A small por-

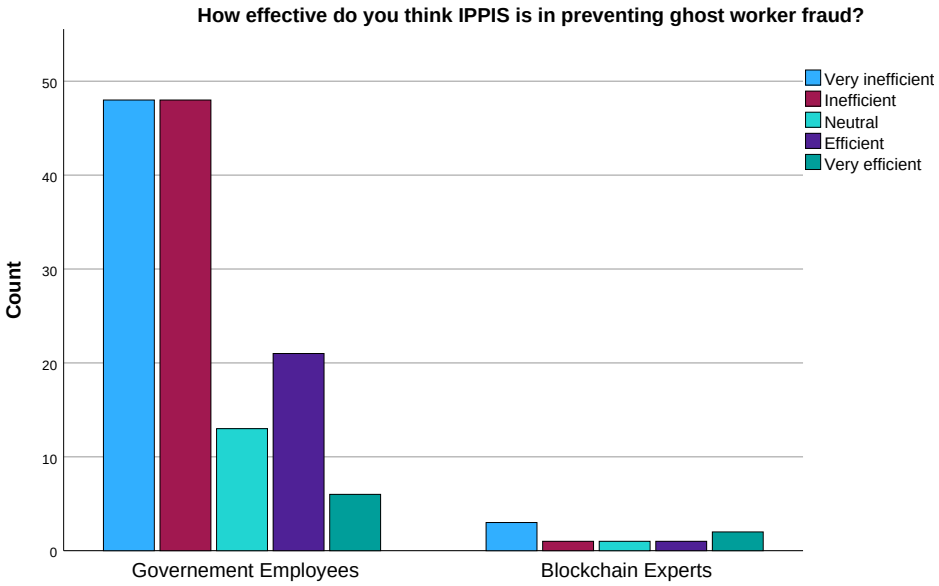


Figure 8.5: How effective do you think IPPIS is in preventing ghost worker fraud?

tion (9.0%) remained neutral. Blockchain experts were less negative but still cautious: 37.5% rated IPPIS as very inefficient, and only 25% viewed it positively. The absence of strong positive ratings among employees, contrasted with the more balanced but limited optimism from experts, suggests a shared scepticism, rooted in operational experience for employees and technical evaluation for experts. Table 8.9 and Figure 8.6

Table 8.9: Q7: How important do you think that multiple agencies should verify and validate every new employee?

| | Government Employees | | Blockchain Experts | | Total | |
|---|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count | % of Total |
| Not important | 0 | 0.0% | 1 | 0.7% | 1 | 0.7% |
| Somewhat important | 33 | 23.1% | 0 | 0.0% | 33 | 23.1% |
| Neutral | 6 | 4.2% | 0 | 0.0% | 6 | 4.2% |
| Important | 28 | 19.6% | 0 | 0.0% | 28 | 19.6% |
| Very important | 68 | 47.6% | 7 | 4.9% | 75 | 52.4% |
| Total | 135 | 94.4% | 8 | 5.6% | 143 | 100.0% |

indicate that respondents widely supported inter-agency coordination as a mechanism

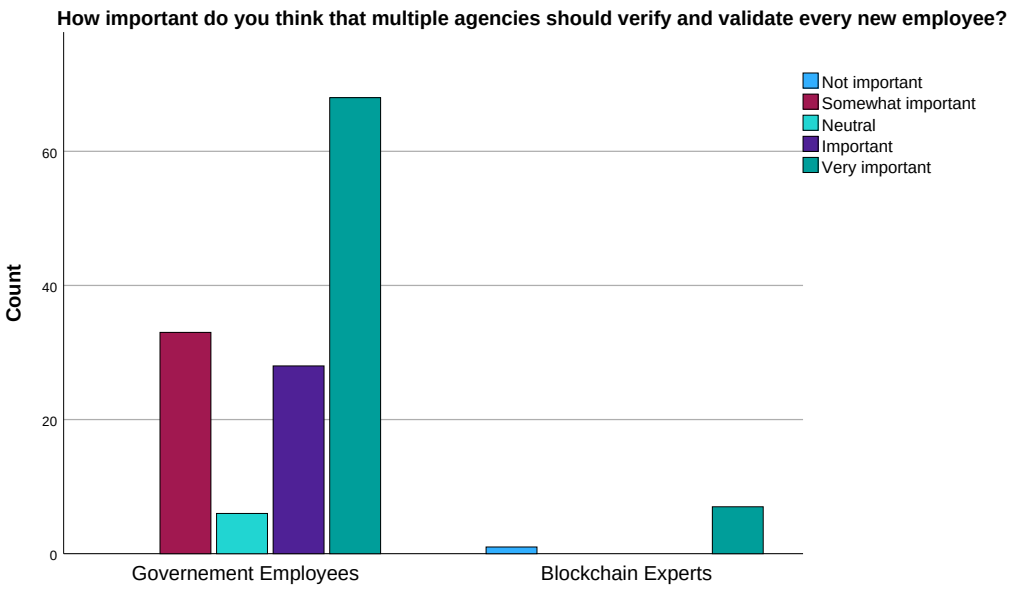


Figure 8.6: How important do you think that multiple agencies should verify and validate every new employee?

to reduce ghost worker fraud. Among government employees, 90.3% rated coordination as somewhat important, important, or very important, with nearly half (47.6%) selecting very important. Blockchain experts unanimously endorsed its importance, with 87.5% rating it very important and none expressing neutrality or disagreement. The slight presence of neutrality and lower ratings among employees suggests practical reservations rooted in bureaucratic experience, while experts demonstrated clear confidence in system-level integration as a solution. Table 8.10 and Figure 8.7 show

Table 8.10: Q8: How effective would real-time verification of new employee records be in reducing ghost worker fraud?

| | Government Employees | | Blockchain Experts | | Total | |
|---|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count | % of Total |
| Slightly effective | 3 | 2.1% | 0 | 0.0% | 3 | 2.1% |
| Moderately effective | 47 | 32.9% | 1 | 0.7% | 48 | 33.6% |
| Very effective | 44 | 30.8% | 2 | 1.4% | 46 | 32.2% |
| Extremely effective | 41 | 28.7% | 5 | 3.5% | 46 | 32.2% |
| Total | 135 | 94.4% | 8 | 5.6% | 143 | 100.0% |

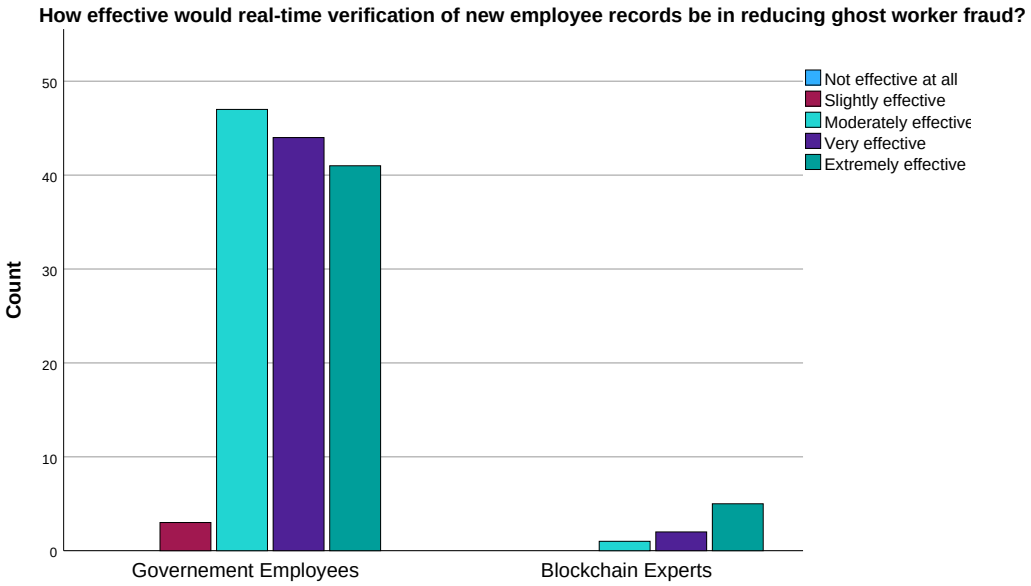


Figure 8.7: How effective would real-time verification of new employee records be in reducing ghost worker fraud?

strong support for real-time verification of employee records as a strategy to reduce ghost worker fraud. Among government employees, 92.4% rated the approach as moderately effective to extremely effective, with 59.5% selecting very or extremely effective. Blockchain experts unanimously endorsed its effectiveness, with 75% choosing the highest rating. The absence of negative responses among experts contrasts with the small minority (2.1%) of employees who viewed the method as only slightly effective. This reflects a shared belief in the value of strong verification process, with experts showing greater confidence likely due to their familiarity with digital validation systems.

Looking at the information in Table 8.11 and Figure 8.8, both groups recognised the value of decentralised data sharing in improving employment record accuracy. Among government employees, 81.2% believed it would "improve somewhat" or "significantly improve" accuracy, while experts unanimously endorsed improvement, with 75% opting for significant gains. The absence of negative ratings among experts contrasts with the small but notable scepticism among employees (13.3% reporting no change or decreased accuracy). This indicates a shared optimism, but with stronger conviction among ex-

Table 8.11: Q9: In your view, how would decentralised data sharing improve the accuracy of employment information across many agencies?

| | Government Employees | | Blockchain Experts | | Total | |
|---|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count | % of Total |
| Decrease accuracy | 7 | 4.9% | 0 | 0.0% | 7 | 4.9% |
| No change | 12 | 8.4% | 0 | 0.0% | 12 | 8.4% |
| Improve somewhat | 65 | 45.5% | 2 | 1.4% | 67 | 46.9% |
| Significantly improve | 51 | 35.7% | 6 | 4.2% | 57 | 39.9% |
| Total | 135 | 94.4% | 8 | 5.6% | 143 | 100.0% |

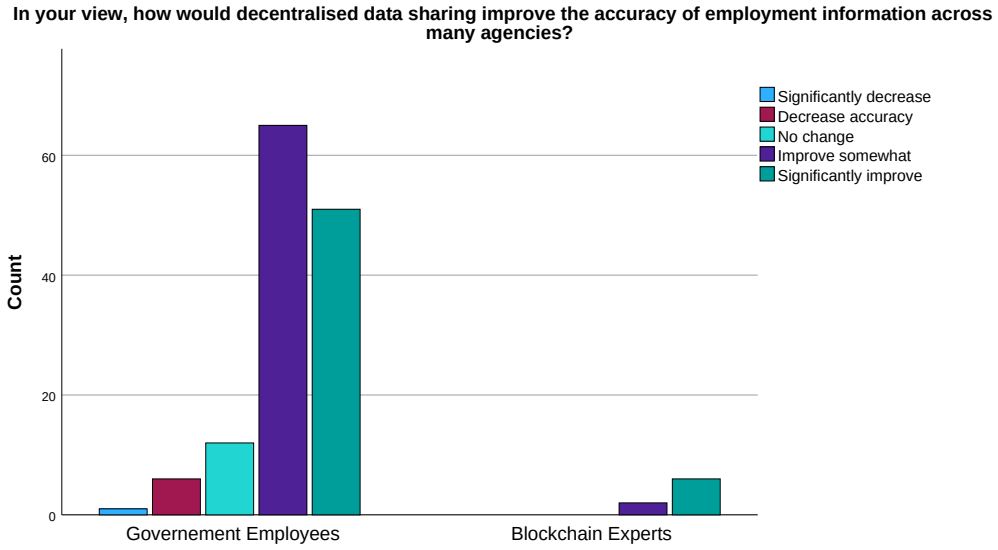


Figure 8.8: In your view, how would decentralised data sharing improve the accuracy of employment information across many agencies?

perts, reflecting their familiarity with decentralised technologies. Confidence levels in

Table 8.12: Q10: How confident are you that real-time verification would contribute in preventing ghost worker fraud?

| | Government Employees | | Blockchain Experts | | Total | |
|---|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count | % of Total |
| Not at all confident | 1 | 0.7% | 0 | 0.0% | 1 | 0.7% |
| Not confident | 14 | 9.8% | 1 | 0.7% | 15 | 10.5% |
| Neutral | 19 | 13.3% | 1 | 0.7% | 20 | 14.0% |
| Confident | 51 | 35.7% | 1 | 0.7% | 52 | 36.4% |
| Very confident | 50 | 35.0% | 5 | 3.5% | 55 | 38.5% |
| Total | 135 | 94.4% | 8 | 5.6% | 143 | 100.0% |

real-time verification were generally high as shown in Table 8.12 and Figure 8.9. Among employees, 70.7% expressed confidence, with 35% reporting they were "very confident." Experts were even more decisive, with 62.5% selecting "very confident" compared to just 12.5% who remained neutral or less. The data shows alignment on the promise of real-time verification, but experts displayed stronger belief in its transformative effect, likely due to greater exposure to technical solutions. Table 8.13 and Figure 8.10

Table 8.13: Q11: Do you think that coordination between agencies (e.g., IPPIS, CBN, Ministries) would reduce fraudulent employment practices?

| | Government Employees | | Blockchain Experts | | Total | |
|---|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count | % of Total |
| No, not at all | 3 | 2.1% | 0 | 0.0% | 3 | 2.1% |
| Not sure | 11 | 7.7% | 1 | 0.7% | 12 | 8.4% |
| Neutral | 8 | 5.6% | 0 | 0.0% | 8 | 5.6% |
| Yes, to some extent | 69 | 48.3% | 2 | 1.4% | 71 | 49.7% |
| Yes, significantly | 44 | 30.8% | 5 | 3.5% | 49 | 34.3% |
| Total | 135 | 94.4% | 8 | 5.6% | 143 | 100.0% |

indicate that respondents widely supported inter-agency coordination as a mechanism to reduce fraudulent practices. Nearly 80% of employees believed coordination would reduce fraud to some extent or significantly, while all experts (100%) shared the same view, with 62.5% rating the effect as significant. Neutrality and uncertainty were higher

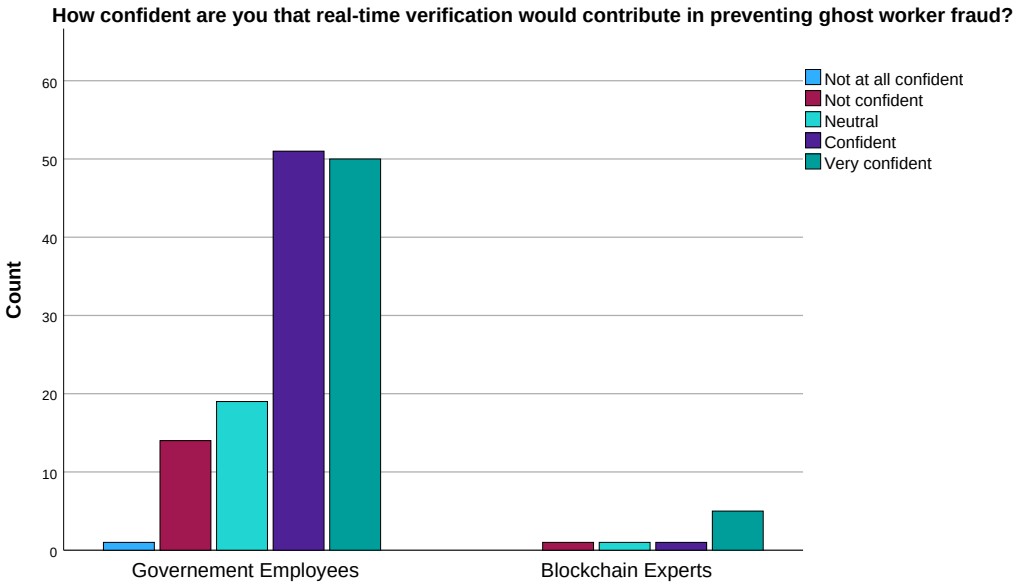


Figure 8.9: How confident are you that real-time verification would contribute in preventing ghost worker fraud?

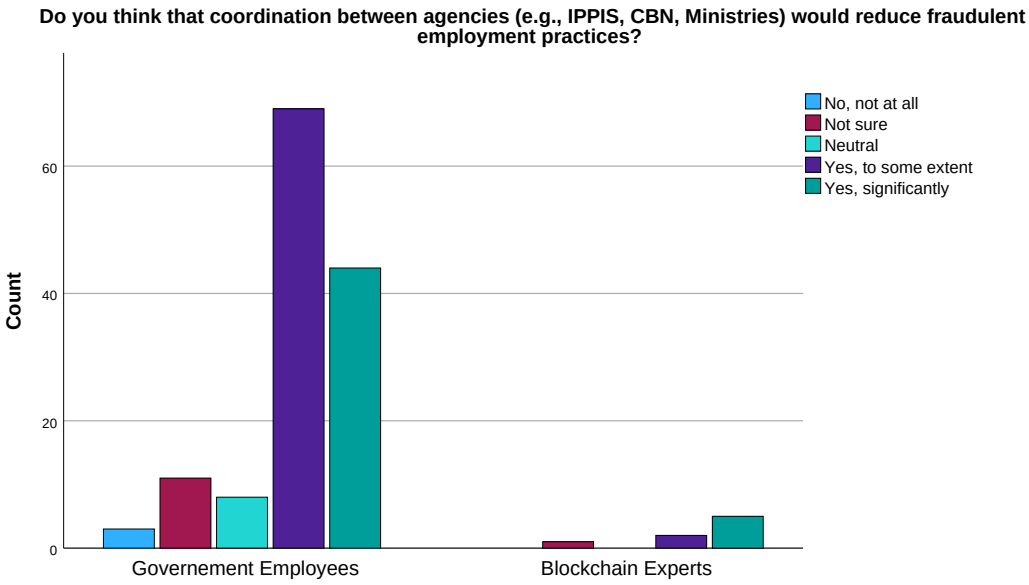


Figure 8.10: Do you think that coordination between agencies (e.g., IPPIS, CBN, Ministries) would reduce fraudulent employment practices?

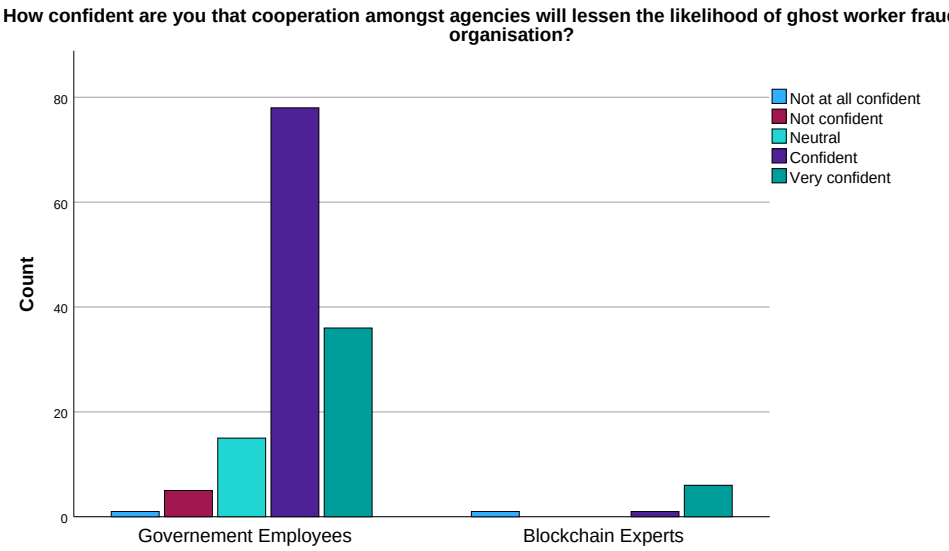


Figure 8.11: How confident are you that cooperation amongst agencies will lessen the likelihood of ghost worker fraud in your organisation?

among employees, pointing to reservations grounded in their experience of bureaucratic inefficiencies. Experts, however, demonstrated confidence in coordination, underscoring the importance of system-level integration. Both groups expressed strong confidence

Table 8.14: Q12: How confident are you that cooperation amongst agencies will lessen the likelihood of ghost worker fraud in your organisation?

| | Government Employees | | Blockchain Experts | | Total |
|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count (% of Total) |
| Not at all confident | 1 | 0.7% | 1 | 0.7% | 2 (1.4%) |
| Not confident | 5 | 3.5% | 0 | 0.0% | 5 (3.5%) |
| Neutral | 15 | 10.5% | 0 | 0.0% | 15 (10.5%) |
| Confident | 78 | 54.5% | 1 | 0.7% | 79 (55.2%) |
| Very confident | 36 | 25.2% | 6 | 4.2% | 42 (29.4%) |
| Total | 135 | 94.4% | 8 | 5.6% | 143 (100%) |

that cooperation among agencies would reduce ghost worker fraud from Table 8.14 and Figure 8.11. For employees, 79.7% were confident or very confident, with a majority favouring the "confident" option. Experts leaned more heavily towards "very

confident" (75%), indicating deeper conviction. This difference suggests that while employees acknowledge cooperation's value, experts anticipate a stronger and more immediate impact. Information in Table 8.15 and Figure 8.12 show that the importance

Table 8.15: Q13: How important is it to have robust access control to employee records during the employment process?

| | Government Employees | | Blockchain Experts | | Total |
|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count (% of Total) |
| Not important | 1 | 0.7% | 0 | 0.0% | 1 (0.7%) |
| Somewhat important | 4 | 2.8% | 0 | 0.0% | 4 (2.8%) |
| Neutral | 12 | 8.4% | 0 | 0.0% | 12 (8.4%) |
| Important | 57 | 39.9% | 0 | 0.0% | 57 (39.9%) |
| Very important | 61 | 42.7% | 8 | 5.6% | 69 (48.3%) |
| Total | 135 | 94.4% | 8 | 5.6% | 143 (100%) |

of access control received overwhelming support. Among employees, 82.6% rated it as important or very important, while experts unanimously agreed, with 100% selecting "very important." This near-consensus reflects a shared recognition that robust access controls are essential safeguards against internal manipulation of employment records. The stronger response from experts suggests a heightened awareness of cyber risks.

Table 8.16: Q14: How important do you believe that restricting access of employee records to authorised staff alone will help to lower internal fraud risks?

| | Government Employees | | Blockchain Experts | | Total |
|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count (% of Total) |
| Not important | 2 | 1.4% | 0 | 0.0% | 2 (1.4%) |
| Somewhat important | 11 | 7.7% | 0 | 0.0% | 11 (7.7%) |
| Neutral | 13 | 9.1% | 2 | 1.4% | 15 (10.5%) |
| Important | 61 | 42.7% | 1 | 0.7% | 62 (43.4%) |
| Very important | 48 | 33.6% | 5 | 3.5% | 53 (37.1%) |
| Total | 135 | 94.4% | 8 | 5.6% | 143 (100%) |

Restricting access to authorised personnel was also seen as critical as shown in Table 8.16 and Figure 8.13. Among employees, 76.3% considered it important or very important, while experts were slightly more emphatic, with 75% choosing "very impor-

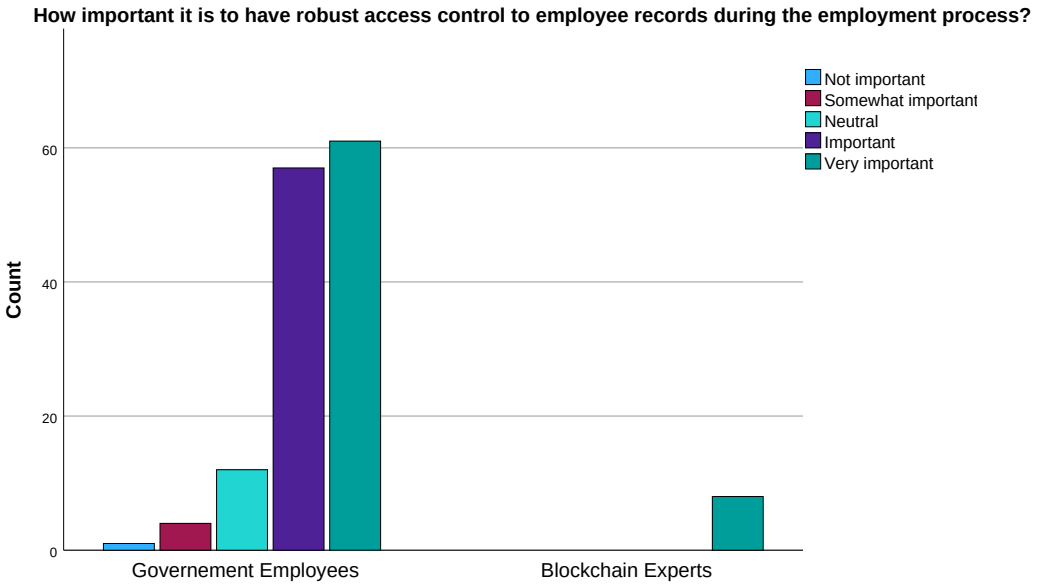


Figure 8.12: How important is it to have robust access control to employee records during the employment process?

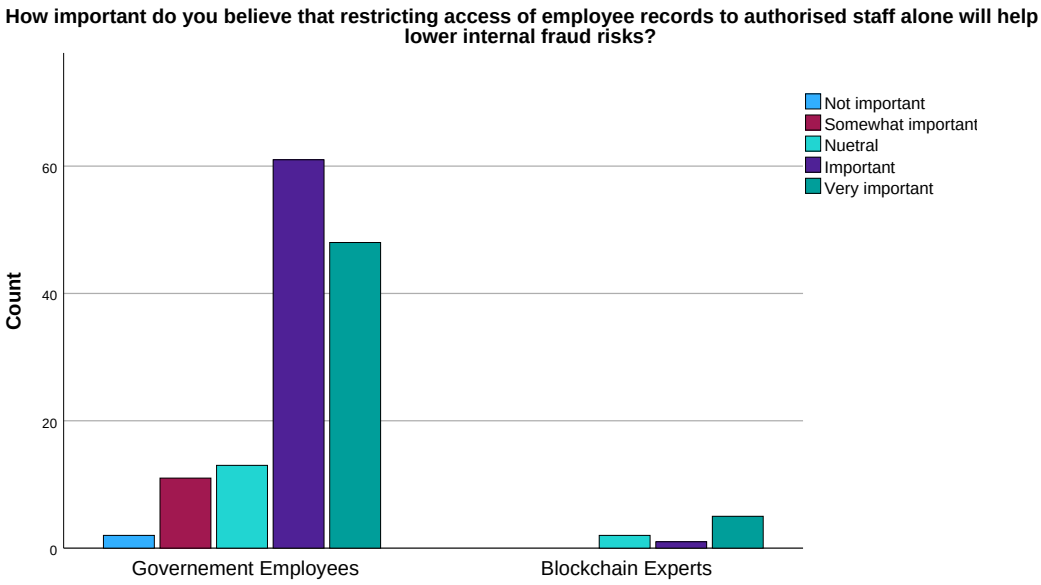


Figure 8.13: How important do you believe that restricting access of employee records to authorised staff alone will help to lower internal fraud risks?

tant." Notably, employees displayed slightly higher neutrality and scepticism (18.2% combined), while experts demonstrated minimal hesitation. These results reinforce the principle of access minimisation as a shared priority for fraud prevention. Table 8.17

Table 8.17: Q15: How confident are you that improved access restrictions will minimise ghost worker fraud?

| | Government Employees | | Blockchain Experts | | Total |
|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count (% of Total) |
| Not at all confident | 1 | 0.7% | 1 | 0.7% | 2 (1.4%) |
| Not confident | 6 | 4.2% | 1 | 0.7% | 7 (4.9%) |
| Neutral | 12 | 8.4% | 1 | 0.7% | 13 (9.1%) |
| Confident | 64 | 44.8% | 1 | 0.7% | 65 (45.5%) |
| Very confident | 52 | 36.4% | 4 | 2.8% | 56 (39.2%) |
| Total | 135 | 94.4% | 8 | 5.6% | 143 (100%) |

and Figure 8.14 reveal that confidence in access restrictions as a fraud mitigation tool was strong across groups. Among employees, 81.2% were confident or very confident, while experts showed less consensus, with responses split across the spectrum but a majority (62.5%) still selecting "very confident." The divergence may reflect employees' practical experience with weak enforcement, while experts project confidence in technological enforcement mechanisms. Feedback systems for reporting inconsisten-

Table 8.18: Q16: Would having a feedback mechanism for reporting inconsistencies in employee records assist discover ghost workers earlier?

| | Government Employees | | Blockchain Experts | | Total |
|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count (% of Total) |
| No, not at all | 1 | 0.7% | 0 | 0.0% | 1 (0.7%) |
| Not sure | 4 | 2.8% | 0 | 0.0% | 4 (2.8%) |
| Neutral | 6 | 4.2% | 0 | 0.0% | 6 (4.2%) |
| Yes, to some extent | 64 | 44.8% | 3 | 2.1% | 67 (46.9%) |
| Yes, significantly | 60 | 42.0% | 5 | 3.5% | 65 (45.5%) |
| Total | 135 | 94.4% | 8 | 5.6% | 143 (100%) |

cies attracted strong approval from Table 8.18 and Figure 8.15. Among employees, 86.8% agreed it would help identify ghost workers, with responses evenly split between

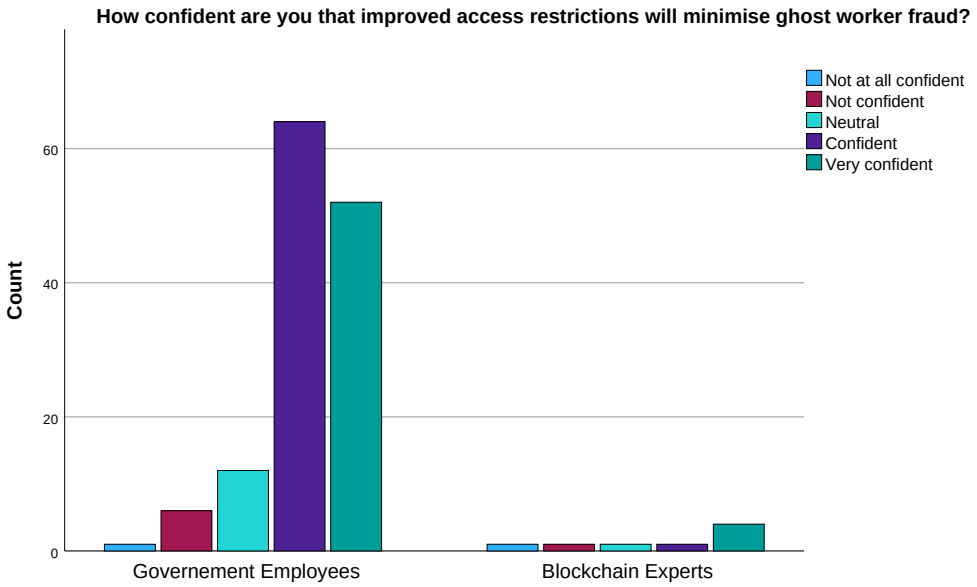


Figure 8.14: How confident are you that improved access restrictions will minimise ghost worker fraud?

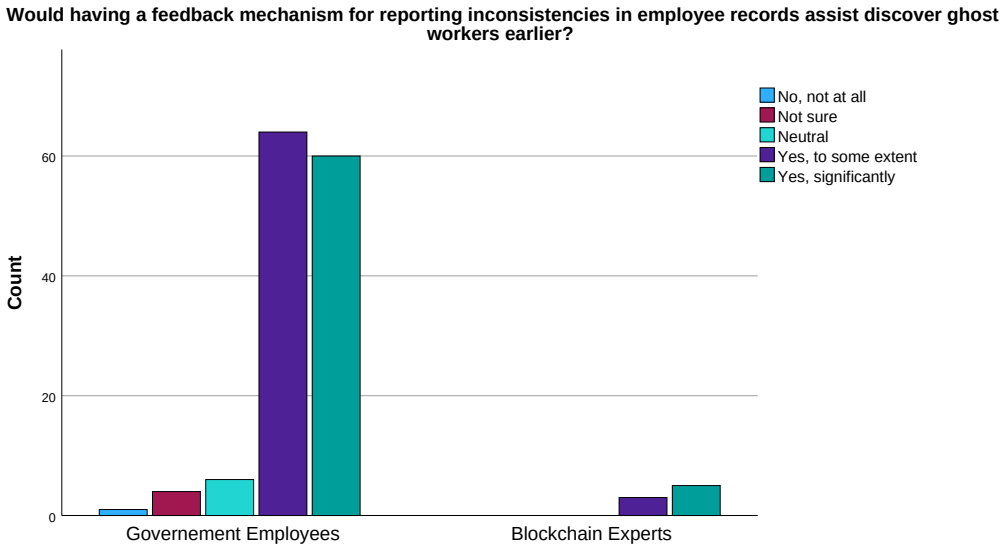


Figure 8.15: Would having a feedback mechanism for reporting inconsistencies in employee records assist discover ghost workers earlier?

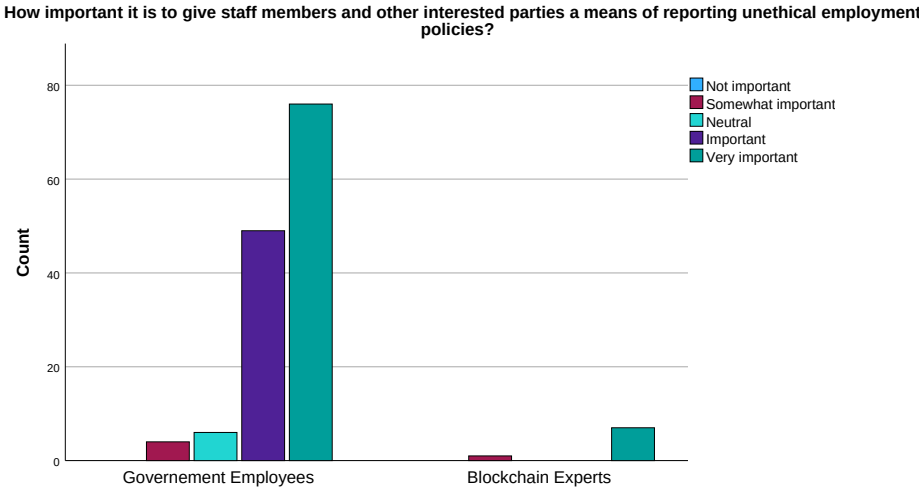


Figure 8.16: How important is it to give staff members and other interested parties a means of reporting unethical employment policies?

"to some extent" and "significantly." Experts unanimously agreed, with 62.5% strongly favouring the "significant" option. This convergence highlights the importance of participatory monitoring tools in strengthening institutional integrity. In Table 8.19

Table 8.19: Q17: How important is it to give staff members and other interested parties a means of reporting unethical employment policies?

| | Government Employees | | Blockchain Experts | | Total |
|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count (% of Total) |
| Somewhat important | 4 | 2.8% | 1 | 0.7% | 5 (3.5%) |
| Neutral | 6 | 4.2% | 0 | 0.0% | 6 (4.2%) |
| Important | 49 | 34.3% | 0 | 0.0% | 49 (34.3%) |
| Very important | 76 | 53.1% | 7 | 4.9% | 83 (58.0%) |
| Total | 135 | 94.4% | 8 | 5.6% | 143 (100%) |

and Figure 8.16, support for reporting channels on unethical practices was overwhelming. Among employees, 87.4% rated them important or very important, with over half choosing the strongest rating. Experts again displayed agreement, with 87.5% selecting "very important." This indicates strong consensus across groups that ethical oversight mechanisms are indispensable for safeguarding integrity. The respondents showed

Table 8.20: Q18: If a feedback system were in place, how likely would staff members or stakeholders disclose irregularities in the system?

| | Government Employees | | Blockchain Experts | | Total |
|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count (% of Total) |
| Very unlikely | 1 | 0.7% | 0 | 0.0% | 1 (0.7%) |
| Unlikely | 3 | 2.1% | 0 | 0.0% | 3 (2.1%) |
| Neutral | 8 | 5.6% | 0 | 0.0% | 8 (5.6%) |
| Likely | 53 | 37.1% | 1 | 0.7% | 54 (37.8%) |
| Very likely | 70 | 49.0% | 7 | 4.9% | 77 (53.8%) |
| Total | 135 | 94.4% | 8 | 5.6% | 143 (100%) |

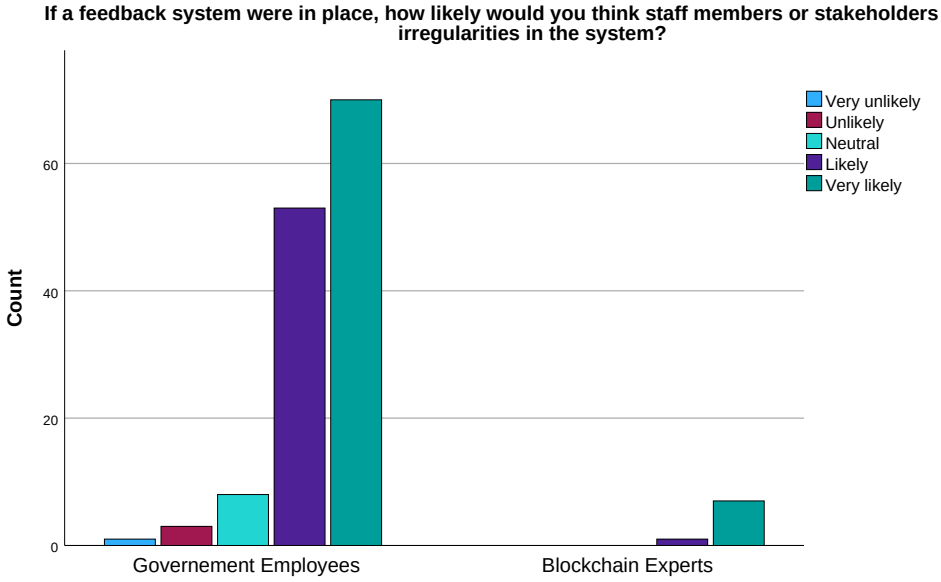


Figure 8.17: If a feedback system were in place, how likely would staff members or stakeholders disclose irregularities in the system?

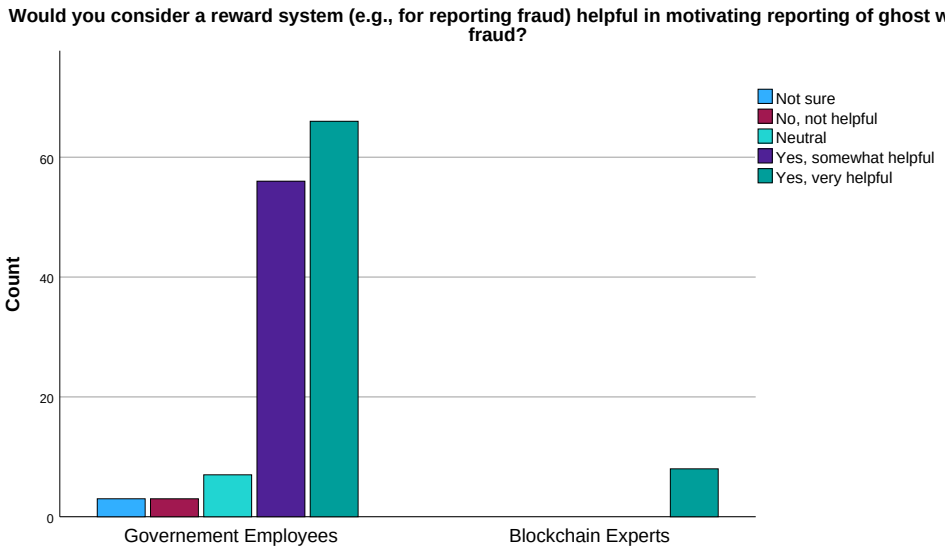


Figure 8.18: Would you consider a reward system (e.g., for reporting fraud) helpful in motivating reporting of ghost worker fraud?

a high willingness to use feedback systems to disclose irregularities as shown in Table 8.20 and Figure 8.17. Among employees, 86.1% reported being likely or very likely to report, with 49% selecting "very likely." Experts unanimously supported disclosure, with 87.5% strongly affirming likelihood. This demonstrates a broad acceptance of feedback channels as effective instruments for accountability. Considering Table 8.21

Table 8.21: Q19: Would you consider a reward system (e.g., for reporting fraud) helpful in motivating reporting of ghost worker fraud?

| | Government Employees | | Blockchain Experts | | Total |
|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count (% of Total) |
| Not sure | 3 | 2.1% | 0 | 0.0% | 3 (2.1%) |
| No, not helpful | 3 | 2.1% | 0 | 0.0% | 3 (2.1%) |
| Neutral | 7 | 4.9% | 0 | 0.0% | 7 (4.9%) |
| Yes, somewhat helpful | 56 | 39.2% | 0 | 0.0% | 56 (39.2%) |
| Yes, very helpful | 66 | 46.2% | 8 | 5.6% | 74 (51.7%) |
| Total | 135 | 94.4% | 8 | 5.6% | 143 (100%) |

and Figure 8.18, among employees, 85.4% rated them somewhat or very helpful, with

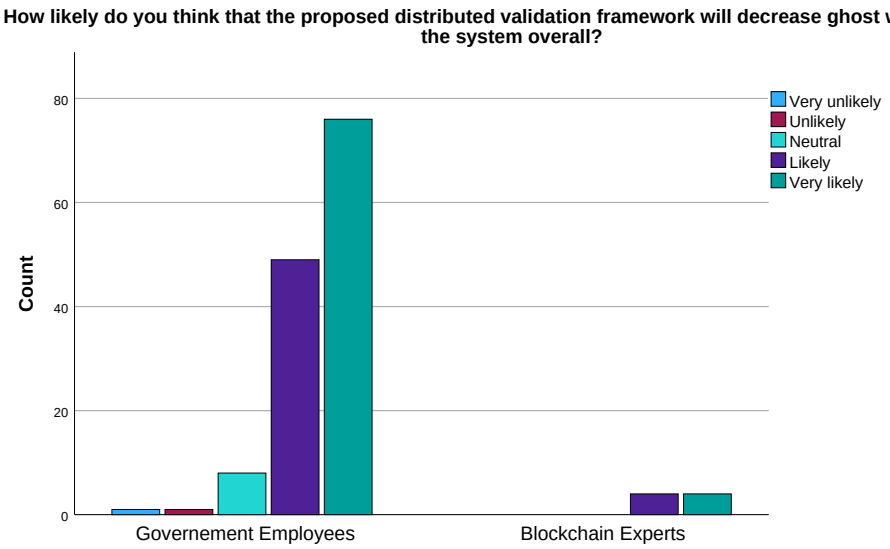


Figure 8.19: How likely do you think that the proposed distributed validation framework will decrease ghost worker fraud overall?

the strongest support for "very helpful" (48.9%). Experts were unanimous, with 100% affirming helpfulness and all selecting the strongest category. This result suggests a convergence on incentives as a critical enabler of whistleblowing and fraud detection. The

Table 8.22: Q20: How likely do you think that the proposed distributed validation framework will decrease ghost worker fraud overall?

| | Government Employees | | Blockchain Experts | | Total |
|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count (% of Total) |
| Very unlikely | 1 | 0.7% | 0 | 0.0% | 1 (0.7%) |
| Unlikely | 1 | 0.7% | 0 | 0.0% | 1 (0.7%) |
| Neutral | 8 | 5.6% | 0 | 0.0% | 8 (5.6%) |
| Likely | 49 | 34.3% | 4 | 2.8% | 53 (37.1%) |
| Very likely | 76 | 53.1% | 4 | 2.8% | 80 (55.9%) |
| Total | 135 | 94.4% | 8 | 5.6% | 143 (100%) |

proposed distributed validation framework was received with strong optimism. Among government employees in Table 8.22 and as shown on Figure 8.19, 87.4% believed it would likely or very likely reduce ghost worker fraud, while experts again unanimously

Table 8.23: Q21: How likely do you believe the proposed approach will improve public sector general integrity of employment processes?

| | Government Employees | | Blockchain Experts | | Total |
|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count (% of Total) |
| Unlikely | 1 | 0.7% | 0 | 0.0% | 1 (0.7%) |
| Neutral | 6 | 4.2% | 0 | 0.0% | 6 (4.2%) |
| Likely | 40 | 28.0% | 2 | 1.4% | 42 (29.4%) |
| Very likely | 88 | 61.5% | 6 | 4.2% | 94 (65.7%) |
| Total | 135 | 94.4% | 8 | 5.6% | 143 (100%) |

Table 8.24: Q22: In your perspective, how will implementing the proposed framework affect the effectiveness of the system's employment verification processes?

| | Government Employees | | Blockchain Experts | | Total |
|---|---|---|---|---|---|
| | Count | % of Total | Count | % of Total | Count (% of Total) |
| No change | 7 | 4.9% | 0 | 0.0% | 7 (4.9%) |
| Improve somewhat | 48 | 33.6% | 2 | 1.4% | 50 (35.0%) |
| Significantly improve | 80 | 55.9% | 6 | 4.2% | 86 (60.1%) |
| Total | 135 | 94.4% | 8 | 5.6% | 143 (100.0%) |

agreed, evenly split between "likely" and "very likely." Neutrality and scepticism were minimal, underscoring broad belief in the framework's potential. In Table 8.23 and Figure 8.20, respondents widely agreed that the framework would strengthen integrity in employment processes. Among employees, 89.5% expected improvements, with 61.5% "very likely." Experts mirrored this optimism, with 75% anticipating integrity gains. This alignment underscores cross-group recognition of the framework's systemic value.

Table 8.24 and Figure 8.20 illustrate broad support for the proposed framework aimed at enhancing employment verification processes. Among government employees, 89.5% viewed the framework as moderately to highly effective, with 55.9% selecting "Significantly improve." This indicates strong institutional confidence in the framework's potential to curb inefficiencies or fraud. On the other hand, blockchain experts showed unanimous support, with 100% indicating improvement and 75% selecting the highest rating. The absence of negative responses among experts contrasts with the 4.9% of government employees who anticipated no change. This disparity suggests that experts,

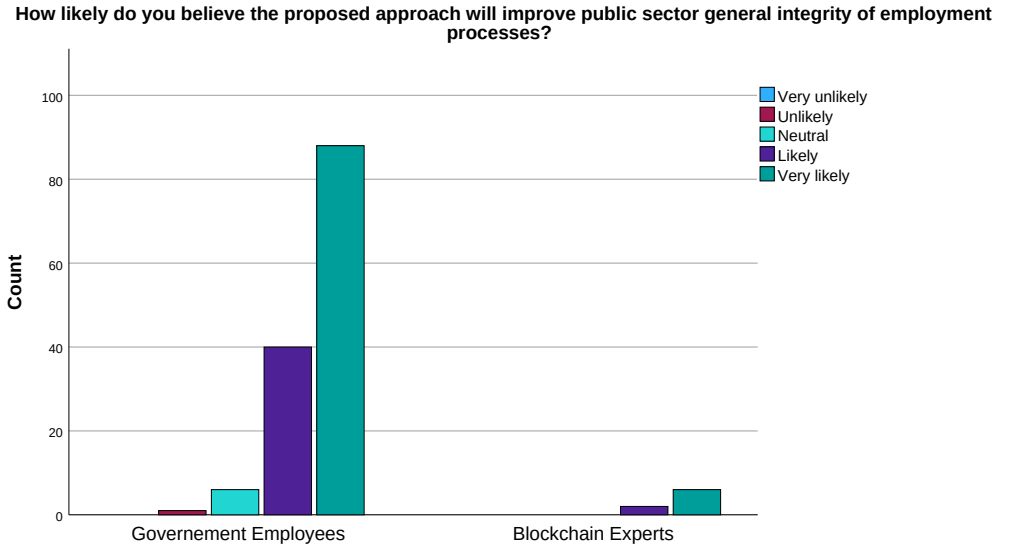


Figure 8.20: How likely do you believe the proposed approach will improve public sector general integrity of employment processes?

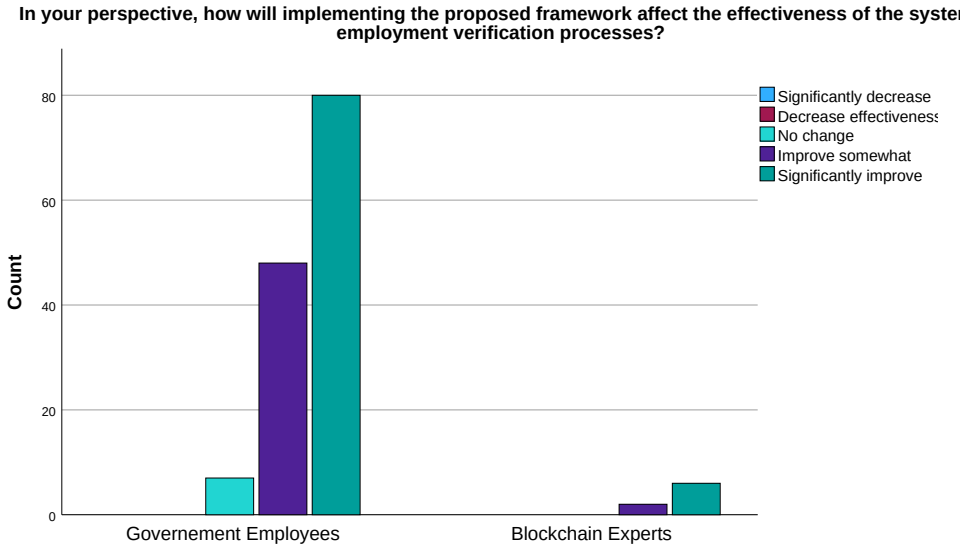


Figure 8.21: In your perspective, how will implementing the proposed framework affect the effectiveness of the system's employment verification processes?

likely due to their deeper understanding of digital systems, have greater confidence in the framework's transformative potential. Overall, 95.1% of all respondents expect the framework to improve effectiveness, reinforcing a shared belief in its value, with experts showing slightly stronger conviction.

### 8.5.1 Analysis of 2024 Survey Findings

To begin with, the demographic profile of respondents revealed that the majority were federal government employees (94.4%), while blockchain experts constituted only 5.6%. This distribution aligns with the study's focus on public sector employment integrity, where government employees are the primary stakeholders. The limited number of blockchain experts reflects the niche but expanding community of blockchain professionals in Nigeria, consistent with recent assessments of the country's digital talent landscape [193]. In the same vein, educationally, the sample was highly qualified: 42.4% held Bachelor's degrees, 24.3% Master's, and 10.4% PhDs. This suggests that respondents were well-equipped to understand employment process, integrity challenges, and to some extent, the conceptual blockchain framework proposed. Compared to earlier studies on civil service capacity [36] [27], these findings indicate a gradual upskilling of Nigeria's public workforce. However, this strong educational profile may introduce a bias toward technically literate staff, potentially underrepresenting the views of lower-level employees who are more vulnerable to fraud-driven exploitation [295]. Secondly, in terms of how IPPIS is generally perceived from the survey, respondents expressed widespread dissatisfaction with the IPPIS ( see Figure 8.2, Figure 8.3, Figure 8.4, and Figure 8.5. This reflects a deep lack of trust in IPPIS's ability to address employment fraud. As daily users, employees are well-positioned to identify operational flaws that may be invisible at the policy level. Studies [50] [20] confirm that centralized payroll systems like IPPIS often create opportunities for manipulation and fail to deliver expected efficiency gains. On the other hand, blockchain experts offered more mixed assessments, rating IPPIS inefficient and an equal proportion finding it efficient. This divergence suggests that technical observers may view IPPIS as a functional centralized database, while employees experience its vulnerabilities firsthand. This dis-

crepancy strengthens the rationale for developing decentralized system to close insider manipulation loopholes while maintaining technical auditability [56]. Again, from the survey result, a significant majority of respondents acknowledged that ghost worker fraud remains prevalent despite IPPIS. Government employees reported awareness of practices. Blockchain experts, though less directly exposed, agreed that centralized systems like IPPIS are inherently vulnerable to insider fraud. Their perspective reinforces the need for architectural reform rather than incremental fixes. The consensus across both groups suggests that ghost worker fraud persists due to structural weaknesses in centralization and inadequate validation protocols [319] [247]. In terms of participants' perceptions on validation mechanisms which is one of the study's core contributions, respondents strongly supported multi-stakeholder verification (see Figure 8.6, Figure 8.10, and Figure 8.11) , favouring that multiple agencies approve new employee entries. This contrasts sharply with IPPIS, where a single HR officer can activate payroll status which is a major vulnerability [247]. Government employees perceived the current IPPIS validation as not sufficiently strong to curtail employment fraud. Blockchain experts emphasized that consensus mechanisms provide cryptographic assurance that fraudulent entries cannot be finalized without majority agreement [56]. This convergence suggests that decentralized validation is both practically desired and technically feasible. Finally, with regards to perceived effectiveness of the proposed framework, most respondents expressed optimism about its potential to address employment fraud in Nigeria (see Figure 8.19, Figure 8.20, and Figure 8.21). The respondents agreed that DEIFP would likely reduce insider manipulation by removing single points of control, and enhance transparency by making employment records verifiable across agencies. This aligns with Christidis and Devetsikiotis who highlight blockchain's potential to automate trust in multi-stakeholder contexts [92]. However, a minor concerns should not be ignored, specifically how validators would be selected, monitored, and prevented from colluding. This signals the need for future refinements in validator governance models.

## 8.6 Conclusion

Both government employees and blockchain experts generally supported the proposed framework, particularly its ability to eliminate ghost worker fraud and promote transparency in the employment process. Blockchain experts, on the other hand, constantly showed greater confidence in the proposed framework, especially regarding the importance of decentralized solutions, strong verification process, and the role of feedback mechanisms in ensuring data accuracy. In contrast, government employees were more sceptical of the current IPPIS system, particularly its effectiveness and transparency. Their concerns regarding its capacity to resolve issues such as ghost worker fraud and enhance employment verification processes. The DEIFP framework is perceived to have great potential in tackling the problems identified with the present IPPIS system. Its decentralized approach, real-time validation, and feedback mechanisms propose a solution for the problems of data transparency and fraud detection. Given the framework's strong reception by both groups, future development and implementation of DEIFP could result in significant changes in public sector employment procedures, boosting both integrity and operational efficiency.

# Chapter 9

# Discussion of findings

Ghost worker fraud remains a widespread challenge across developing countries' public sectors [252] [247] [377] [15] [239]. Prior studies ([247] [124] [292]) have revealed how centralized systems like the IPPIS are susceptible to manipulation due to limited oversight, access control issues, and insufficient audit trails. Blockchain has been increasingly proposed as a remedy for such issues. Christidis and Devetsikiotis and Zheng et al. argue that distributed ledger technologies can improve accountability, eliminate central points of failure, and enhance data verifiability [92] [444]. This thesis, building on that foundation, evaluates the DEIFP framework as a blockchain-based architecture for curbing ghost worker fraud in Nigeria. The quantitative results of the 2024 survey and the case study evaluation are discussed in this chapter. The two main study themes: (1) the ineffectiveness of IPPIS in reducing ghost worker fraud and (2) the potential effectiveness of the DEIFP framework in addressing the identified systemic weaknesses.

## 9.1 Evaluation of the DEIFP framework

The DEIFP framework received strong support from respondents in the 2024 survey. Its three major features; decentralized validation, verification, and multi-stakeholder collaboration were seen as key improvements over IPPIS. Participants valued the fact that the DEIFP removes sole authority from a single managing body and involves institutions like the CBN, the Office of the Auditor General, and other stakeholders as validators. This supports findings from Pothuri, who emphasized decentralized consensus mechanisms combined with can effectively detect fraud in distributed systems [313], also Goel and Saunoris argued that decentralization of government functions, including

government employment process, can reduce shadow economy prevalence, with physical decentralization being particularly effective against widespread irregular activities [152]. The DEIFP framework was proposed as a solution to IPPIS's challenges. Employees in the 2024 study generally supported the concept of decentralized validation in employment management. The benefits of the DEIFP framework as revealed by the 2024 survey respondents are discussed in this part. First, the distributed data-sharing approach of the DEIFP framework was among its main components that survey participants most valued. DEIFP would include multiple stakeholders in the validation process, including government agencies and regulatory bodies. This is unlike IPPIS, which is centralized and under management by one body. In the proposed DEIFP framework, there is no single entity as a sole authority over employment data; this method greatly lowers the possibility of fraud. This decentralized strategy improves accountability and transparency. Secondly, another main advantage of the proposed DEIFP system was its supposed ability to check and verify employee information before final approval.

In addition, respondents evaluated the DEIFP framework's emphasis on collaboration among multiple stakeholders positively. This multi-stakeholder strategy guarantees that data of employees is vetted on several platforms, thereby making it far more difficult for fraudulent employees to go unnoticed or be misrepresented. With all of this, the survey indicates that by addressing the basic flaws of IPPIS, the DEIFP framework has great potential to enhance the integrity of the employment process and reduce ghost worker fraud.

### 9.1.1 Case study analysis

The case studies examined in this study show the systematic flaws in current payroll and employment systems where fraudsters took advantage of their deficiencies, including poor access control and insufficient monitoring. These defects let ghost workers be included into payrolls, therefore causing large financial losses. As stated in Chapter 7, a system having DEIFP features could have avoided these fraudulent activities by guaranteeing that employment and payroll record were always verified by different

parties before approval.

Lack of verification and appropriate data validation among agencies gave criminals chances to alter payroll systems without detection. Verification and cross-agency cooperation of the DEIFP framework would have found disparities in personnel records as soon as they were entered, therefore preventing the processing of fraudulent inputs. This distributed approach would have made it significantly more difficult for someone to take advantage of system flaws without being discovered. Furthermore, as discussed in 7, poor internal controls and inadequate verification methods let fraud continue in various different forms. These examples underscore the limitations of IPPIS, consistent with O. Samuel and Augustine [351]. By incorporating several stakeholders in the validation process, the DEIFP framework could solve these problems and ensure transparency.

### 9.1.2 Link between IPPIS perception and the DEIFP framework

The data from both the quantitative and qualitative surveys suggest a strong link between dissatisfaction with IPPIS and support for the DEIFP framework. Employees who voiced dissatisfaction with IPPIS' inefficiencies saw the DEIFP as a potential solution to these issues.

It was observed that those who felt that IPPIS was ineffective in addressing ghost worker fraud who were not satisfied were more likely to support the DEIFP approach. Employees' inclination for more transparency and accountability in the payroll and employment system led them to support a distributed solution whereby several independent validators verify employment data. This reflects findings of Druschel, where distributed accountability increases system credibility [119]. Also, respondents who considered IPPIS as a failing solution were more hopeful about the possibility of DEIFP to offer a more efficient framework for stopping fraud. This confidence was mostly due to the DEIFP's proposed capacity to incorporate many layers of verification and control, making it more resistant to fraud.

The link between employee dissatisfaction with IPPIS and support for DEIFP emphasizes the critical need for reform in public sector payroll and employment systems.

It emphasizes that IPPIS's failure to meet expectations has produced a conducive environment to other alternatives.

### 9.1.3 Divergence in Perceptions: Blockchain Experts vs. Government Employees

An interesting pattern emerged in the 2024 survey analysis. The survey results clearly indicate this divergence, however, the underlying reasons were not directly examined in this study and therefore can only be interpreted cautiously. Several possible explanations may be considered:

1. Limited insider experience: Some experts not working within Nigeria's public sector may lack direct exposure to IPPIS's limitations.
2. Technical optimism bias: Experts may have evaluated IPPIS based on its intention, not its operational flaws.
3. Misunderstanding IPPIS's scope: Some may conflate it with broader digital initiatives.
4. Employee frustrations: Daily users experience operational delays, errors, and inefficiencies that inform their skepticism.

These interpretations remain speculative and highlight the importance of incorporating user-centered evaluation when assessing digital public-sector systems.

## 9.2 Limitations of the Study

This study has several limitations:

1. Survey design used the same questions for two very different participant groups. Government employees may lack technical blockchain expertise, while blockchain experts may not fully grasp IPPIS operational dynamics. While this approach enabled comparative analysis across groups, it may have limited the depth of insight obtainable from each category. A more tailored instrument for each group

could have captured technical depth from experts and operational shade from employees more effectively.

2. Even though DEIFP framework was clearly explained before answering the questions, but comprehension levels varied, particularly among non-technical participants. Variations in comprehension may have influenced how certain questions were interpreted, potentially affecting response consistency. Although explanatory materials were provided, alternative methods such as follow-up interviews or interactive workshops could have enhanced understanding.

3. 2021 survey results were not used directly in DEIFP design, which could have enriched the design if applied earlier. The temporal separation between the 2021 findings and the framework development meant that some early insights were not systematically embedded into the initial design phase. Integrating these findings earlier may have strengthened certain structural or governance components of the framework.

4. No working prototype was implemented. The DEIFP framework was evaluated conceptually through surveys and case studies but not tested in a live operational environment. This limits empirical validation of functionality, performance, usability, and integration challenges that might emerge during actual deployment. Even though conceptual and case-based evaluation provided theoretical and contextual validation, it does not substitute for real-world system testing.

These constraints will guide future refinement or implementation of the framework.

## 9.3 Conclusion

This chapter has provided an examination of the results from qualitative case studies as well as quantitative surveys. The DEIFP framework was strongly supported by survey participants as a viable alternative. Its distributed architecture, validation tools, and emphasis on stakeholder cooperation combine to provide a possible solution for the IPPIS issues. The DEIFP structure is seen to have considerable potential

to greatly reduce fraud and boost government employment and payroll system transparency. Dissatisfaction with IPPIS has created an opportunity to consider DEIFP as an alternate framework. Staff members who strongly supported distributed validation are looking for a more transparent, safe, and collaborative employment and payroll handling system. Lastly, while IPPIS has been a great development, it is clear that the persistent difficulties of ghost worker fraud necessitate a shift to a more distributed and collaborative system, such as DEIFP.

# Chapter 10

# Future work

The potential for significant improvements in this research is substantial and spans numerous dimensions, depending on time, funding availability, stakeholder engagement, and technological evolution. Some improvements can be achieved through incremental adjustments to the underlying structure, while others may require entirely novel implementations and inter-agency coordination. This chapter outlines strategic directions for advancing the DEIFP framework, with emphasis on practical extensions, integration of intelligent systems, scalability and interoperability considerations, and regulatory alignment. The suggestions are grounded in real-world use cases and existing research.

## 10.1 Direct extensions

One of the most pressing areas for future research is the real-world implementation of the proposed DEIFP framework within selected government institutions. The deployment would allow a comprehensive assessment of operational efficiency, scalability, resilience, and fraud-reduction potential under real administrative conditions. Key actions include:

1. Pilot implementation in public institutions: This phase should include testbeds in select ministries or government agencies, evaluating metrics such as validator performance, transaction throughput, and fraud detection rate.

2. Training and capacity-building: Developing training programs for HR officers, IT administrators, and compliance teams to ensure the secure and effective operation of the DEIFP system.

3. Validator network expansion: Including additional entities like anti-corruption

agencies, the judiciary, and unions can decentralize verification, boosting system credibility and reducing risks of collusion.

4. Dashboards for transparency: Developing role-based access dashboards for auditors, managers, and observers could enhance usability and allow near real-time insights into hiring and payroll activity.

5. Integration of machine learning (ML): Incorporating ML for fraud detection is a critical next step. For instance, anomaly detection models like Isolation Forests or Autoencoders can learn patterns of legitimate payroll behavior and flag deviations for human review. ML has been successfully used in similar contexts such as insurance fraud detection and financial fraud analytics.

## 10.2 New approaches

Although the focus of this study has been the validation of new hires, future research could broaden the application of the DEIFP framework to other components of public sector human resource management, including performance evaluations and promotions where Smart contracts could automate the linking of validated performance metrics to promotion eligibility, increasing transparency and meritocracy. In addition, payroll disbursement and leave management should be another new approach by integrating bank APIs or CBDC systems (e.g., Nigeria's eNaira) with the DEIFP could create a traceable link between verified employment records and payments.

### 10.2.1 Interoperability and scalability

Scalability and interoperability are two key challenges in blockchain adoption. First, interoperability which entails ensuring DEIFP can work with existing government systems (e.g., NIMC, tax databases, pension registries) requires the use of standardized APIs and data exchange protocols. Frameworks such as Hyperledger Cactus provide examples of cross-platform data sharing. Secondly, scalability enhancements, the ethereum-based networks can face bottlenecks as the user base grows. Future work should explore

Layer 2 solutions like rollups or sharding, as well as evaluating alternative consensus mechanisms that offer higher throughput, such as HotStuff.

### 10.2.2 Policy and regulatory implications

For any blockchain deployment in government, legal and institutional alignment is vital. First, policy co-creation, where researchers and technologists should co-develop regulatory sandboxes with agencies like the Federal Civil Service Commission (FCSC) and the National Identity Management Commission (NIMC). Secondly, the legal frameworks where legislative support is required to recognize blockchain-based digital signatures, smart contracts, and data integrity proofs as legally binding under Nigerian law. And lastly, the ethical governance, DEIFP must also embed privacy-by-design, data minimization, and redress mechanisms to align with national data protection regulations (NDPR) and international standards like GDPR.

## 10.3 Conclusion

While the DEIFP framework shows promise in enhancing payroll integrity, fraud resistance, and multi-agency collaboration, this chapter outlines how it can be further improved and adapted to real-world constraints. Key directions include deployment in live environments and training of stakeholders, enhancing analytics using machine learning for anomaly detection, extending scope to cover the full HR lifecycle, addressing scalability and interoperability through blockchain-layer improvements, and aligning system design with evolving legal and policy landscapes. These areas will not only improve the robustness of the framework but also lay the groundwork for sustainable digital transformation in public service delivery.

# Chapter 11

# Conclusion

## 11.1 Summary of findings

This research has delved into the problem of ghost worker fraud within Nigeria's public sector and explored ways in which blockchain technology could address the weaknesses in IPPIS. Through a combination of quantitative surveys, qualitative case studies, and the development of the DEIFP framework, several key findings have been highlighted. The following are some of the most important key findings from the research:

**Ineffectiveness of IPPIS in preventing fraud:** The research revealed that IPPIS, despite its initial promise, has been largely ineffective in eliminating ghost worker fraud. The system's centralized structure, lack of strong verification, and weak cross-agency collaboration have created significant vulnerabilities that fraudsters have exploited. Both survey results and case studies underscored the persistence of these weaknesses, which have allowed fraudulent activities to thrive within the system.

**Potential of the DEIFP framework:** The proposed DEIFP framework, based on blockchain technology, offers a decentralized solution to combat these systemic problems. By incorporating strong verification mechanism, stakeholder collaboration, and immutable data records, DEIFP could address some of the weaknesses of the IPPIS regarding the employment process. The framework will ensure that no single entity has exclusive control over payroll data, enhancing transparency, accountability, and security.

**Proposed use of IPFS for data integrity:** The InterPlanetary File System (IPFS) was proposed to be utilized in the research project in order to generate hash documents

containing information about prospective employees. This was done in order to ensure full data integrity. Whenever the Head of Service (HoS) enters the information about an employee, for instance, IPFS generates a unique hash that represents the information. This hash is then used as a reference for validation, which ensures that the data will remain consistent and unchangeable during the entire process.

**Enhanced security and transparency:** The immutable ledger of the blockchain provides a secure and transparent record of all transactions, which contributes to the blockchain's overall security and transparency. Within the scope of the study, the information of each validated employee will be recorded on the blockchain, where stakeholders will have the same records. This will result in the creation of a history that will be both auditable and immutable, allowing other parties such as auditors, police, the judiciary, and the EFCC to examine.

## 11.2 Practical implications

The results of this study will have practical implications for the Nigerian public sector as well as for other governments that are confronted with issues in employment and payroll administration that are similar to those in Nigeria. The DEIFP framework has the potential to transform the way government payroll systems are operated by bringing transparency, accountability, and security. The following are the key practical implications:

**Improved employment verification processes:** Because of the decentralized nature of the DEIFP system, it is guaranteed that no single entity will have complete control over the data regarding payroll and employment. The participation of a number of different stakeholders in the validation process minimizes the likelihood that fraudulent individuals will be able to falsify records. The integrity of the employment system as a whole will be improved, as well as the level of transparency, from this method.

**Reduction of fraud and increased transparency:** Blockchain technology, as the backbone of the DEIFP system, creates an immutable record of transactions, making it harder for unauthorized modifications to get through. This transparency not only enhances accountability but also serves as a deterrent to fraudsters, as they are aware that any fraudulent activity will be observable and traceable.

**Policy and regulatory change:** A collaborative effort between policymakers and regulatory authorities would be required in order to guarantee that the DEIFP framework is implemented in a manner that is in accordance with the laws and regulations that are now in place. As part of this process, employment legislation may need to be updated, new policies may need to be implemented, and a legal framework supporting blockchain-based payroll systems may need to be established.

**Capacity building and institutional support:** Government institutions must significantly increase their capability in order to execute the DEIFP framework in practice. This includes teaching staff how to use the system and providing continuing support to ensure that it functions properly if implemented. The system will need to be managed and monitored by a specialized team after it is deployed.

## 11.3 Contributions to knowledge

This research has made significant contributions to the study of fraud prevention in public sector payroll and employment systems. It proposes the DEIFP framework as a novel solution to ghost worker fraud and highlights its potential application in other sectors facing similar challenges. Some of its significant contributions to the body of knowledge include:

**Development of the DEIFP Framework:** The primary contribution of this study lies in the design and development of the DEIFP framework. This framework could reduce the risk of fraud and increase transparency in the employment process by enabling decentralized data validation. By decentralizing the validation of employment data, the

DEIFP framework will ensure that no single entity has control over the process, thus reducing opportunities for fraud. The decentralized nature of the framework also fosters greater accountability, as multiple independent agencies could confirm employment records. These evaluations highlight how the framework could transform employment verification and significantly reduce the risk of ghost worker fraud.

**Blockchain-Driven framework for public sector:** The dissertation introduces a blockchain-based framework for decentralized validation of employment records. While blockchain has been widely discussed in financial systems, its application in public sector employment systems remains underexplored [344]. By adopting Ethereum Besu, this research introduces an innovative way to decentralize data validation, ensuring greater security and accuracy in the employment records management process. This approach not only reduces the risk of fraudulent activities like ghost worker fraud but also enhances the trustworthiness of the entire employment system. This is the first application of Ethereum Besu for public sector employment systems, showcasing its potential for improving both transparency and efficiency in public service management.

**Advancing Blockchain Adoption in the Public Sector:** This research contributes to the growing body of work advocating for blockchain adoption in the governance sector. By demonstrating the potential of blockchain to enhance transparency and reduce fraud particularly in employment verification, this study advances the understanding and application of blockchain technology in public administration. Blockchain has the ability to provide immutable records that cannot be altered or tampered with, offering a higher level of security than traditional systems. Furthermore, blockchain could provide practical verification process and cross-agency collaboration, which are key in mitigating the problem of ghost workers. This study demonstrates how blockchain technology could provide a secure and efficient solution to the challenges facing the public sector.

**Interdisciplinary Approach:** My research integrates insights from information systems, blockchain technology, public administration, and fraud prevention, offering a

comprehensive approach to tackling ghost worker fraud. By combining expertise from multiple fields, the DEIFP framework provides a holistic solution that addresses the technological, administrative, and ethical aspects of fraud prevention. This interdisciplinary approach ensures that the framework is not only technically sound but also practical for implementation within public sector organizations.

**Framework for broader applications:** The approaches in this research could be applied to broader applications or other businesses that require verification processes that are both secure and transparent. The applicability of blockchain technology to data integrity and trust-based situations makes this extension possible. For instance, similar blockchain frameworks could guarantee product authenticity in supply chain management by offering an immutable record of the product's journey from manufacturer to consumer [67]. This has the potential to reduce instances of counterfeiting and increase confidence among multiple parties.

In a similar vein, blockchain technology has the potential to play a significant part in the prevention of fraud in the financial sector by guaranteeing that transaction records are both transparent and tamper-proof. Blockchain technology has already advanced significantly in several sectors, according to research. For instance, Provenance, a firm that uses blockchain technology to increase transparency of its supply chain, has successfully established a system that monitors the histories and origins of products [381]. In addition, the Quorum blockchain that is used by JPMorgan Chase has proved the potential of blockchain technology to improve the security and effectiveness of financial transactions [373]. These blockchain frameworks could be adopted and customized by other businesses to suit their unique requirements, hence facilitating wider applications and innovations across several sectors. This could be achieved by utilizing the technologies and insights acquired from this study.

## 11.4 Recommendation

Based on the findings and analysis reported in this research, the following recommendations are offered:

**Implementation of pilot projects:** To validate the DEIFP framework's effectiveness, pilot initiatives must be implemented immediately within chosen government entities. These pilot studies will give important information on how the framework functions in real-world contexts, as well as an opportunity to identify any implementation issues. This phase will further enhance the framework to more effectively meet the practical requirements of many government departments.

**Collaboration with stakeholders:** Encouraging collaboration among diverse stakeholders, including governmental entities, regulatory authorities, and blockchain experts is recommended. This collaborative effort among multiple stakeholders will guarantee that the framework is resilient, efficient, and in accordance with national and international standards. Consistent collaboration will guarantee that the framework stays flexible and expandable as new challenges emerge.

**Policy and regulatory alignment:** The DEIFP framework must be developed to adhere to legal and regulatory criteria. Future development must entail collaboration with legislators and legal professionals to guarantee that blockchain-based systems align with current legislation. This will promote a trusting atmosphere and make it easier for blockchain to be widely used in public sector systems.

## 11.5 Conclusion

In conclusion, this research has successfully demonstrated the potential of blockchain technology to address the issue of ghost worker fraud in Nigeria public sector employment systems. The DEIFP framework would provide a decentralized, transparent, and secure alternative to traditional payroll and employment system inefficiencies, lowering the risk of fraud and enhancing public fund management. However, successful implementation of the DEIFP framework will necessitate dealing with legal and regulatory issues. Future research and real-world testing will be critical for improving the system and achieving widespread adoption across government departments. The proposed DEIFP could serve as a model for other industries or governments with similar

centralized issues seeking to decrease fraud and improve transparency. The ultimate goal is to establish a more transparent, secure, and efficient system for managing public sector employment in Nigeria, ensuring that public resources are spent effectively and that people have better confidence in the government's competence to manage public monies. Blockchain technology, through frameworks like DEIFP, would provide a strong instrument for achieving these goals and paving the way for a new era of governance.

# Bibliography


[1] Abbas, Q. E., & Sung-Bong, J. (2019). A survey of blockchain and its applications. *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, 001–003. https://doi.org/10.1109/ICAIIC.2019.8669067 (cit. on p. 35).

[2] Abdella, J., Tari, Z., Anwar, A., Mahmood, A., & Han, F. (2021). An architecture and performance evaluation of blockchain-based peer-to-peer energy trading. *IEEE Transactions on Smart Grid*, *12*(4), 3364–3378. https://doi.org/10.1109/TSG.2021.3056147 (cit. on pp. 113, 128).

[3] AbdulRasheed, A., Babaita, I. S., & Yinusa, M. A. (2012). Fraud and financial crimes prevention and control in Nigeria: A sociological analysis. *International Journal of Asian Social Science*, *2*(3), 214–219. https://ideas.repec.org/a/asi/ijoass/v2y2012i3p214-219id2175.html (cit. on p. 1).

[4] Abdulsalam Nasiru, K., Kabir, N., Sani, I., Jafaru Abdu, G., & Ubandawaki, L. I. (2020). Integrated Personnel and Payroll Information System (IPPIS) and transparency in government payroll administration in Nigerian Civil Service: A unique approach. *Asian Journal of Economics, Business and Accounting*, 1–8. https://doi.org/10.9734/ajeba/2020/v19i330303 (cit. on p. 24).

[5] Abraham, I., Asharov, G., & Yanai, A. (2022). Efficient perfectly secure computation with optimal resilience. *Journal of Cryptology*, *35*(4), 27. https://doi.org/10.1007/s00145-022-09434-2 (cit. on p. 28).

[6] Abubakar, M., Onyeashie, B. I., Wadhaj, I., Leimich, P., Ali, H., & Buchanan, W. J. (2024). A systematic review of the blockchain technology security challenges and threats classification. *2024 6th International Conference on Blockchain Computing and Applications (BCCA)*, 684–697. https://ieeexplore.ieee.org/abstract/document/10844455/ (cit. on p. 29).

[7] Abu-Elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., & Abd-Alrazaq, A. (2020). The benefits and threats of blockchain technology in healthcare: A scop-

ing review [Publisher: Elsevier]. *International Journal of Medical Informatics*, 104246. https://doi.org/10.1016/j.ijmedinf.2020.104246 (cit. on p. 29).

[8] Acosta, J. D., & Brooks, S. (2021). Descriptive statistics are powerful tools for organizational research practitioners [Publisher: Cambridge University Press]. *Industrial and Organizational Psychology*, *14*(4), 481–485. https://www.cambridge.org/core/journals/industrial-and-organizational-psychology/article/descriptive-statistics-are-powerful-tools-for-organizational-research-practitioners/ (cit. on p. 86).

[9] Adams, C., & Lloyd, S. (2003). *Understanding PKI: Concepts, standards, and deployment considerations*. Addison-Wesley Professional. (Cit. on p. 27).

[10] Agi, M. A. N., & Jha, A. K. (2022). Blockchain technology in the supply chain: An integrated theoretical perspective of organizational adoption. *International Journal of Production Economics*, *247*, 108458. https://doi.org/10.1016/j.ijpe.2022.108458 (cit. on p. 67).

[11] Aguirre, S., & Rodriguez, A. (2017). Automation of a business process using Robotic Process Automation (RPA): A case study [Series Title: Communications in Computer and Information Science]. In J. C. Figueroa-García, E. R. López-Santana, J. L. Villa-Ramírez, & R. Ferro-Escobar (Eds.), *Applied Computer Sciences in Engineering* (pp. 65–71, Vol. 742). Springer International Publishing. https://doi.org/10.1007/978-3-319-66963-2_7 (cit. on p. 27).

[12] Ahmad, D., Lutfiani, N., Ahmad, A. D. A. R., Rahardja, U., & Aini, Q. (2021). Blockchain technology immutability framework design in e-government. *Jurnal Administrasi Publik (Public Administration Journal)*, *11*(1), 32–41. https://doi.org/10.31289/jap.v11i1.4310 (cit. on pp. 118, 125).

[13] Akbar, R. N., Zakaria, A., & Prihatni, R. (2022). Financial statement analysis of Fraud with Hexagon Theory fraud approach. *Jurnal Akuntansi, Perpajakan Dan Auditing*, *3*(1), 137–161. http://pub.unj.ac.id/journal/index.php/japa (cit. on p. 62).

[14] Akshita, V., Dhanush, S., Dikshitha, A., & Krishna Kumar, V. (2021). Blockchain based covid vaccine booking and vaccine management system. *2021 2nd Inter-*

*national Conference on Smart Electronics and Communication (ICOSEC)*, 1–7. https://doi.org/10.1109/ICOSEC51865.2021.9591965 (cit. on p. 128).

[15] Al Bashiri, M. A. (2019). Economic confidence building measures–civil servant salaries. *Policy Brief*, (11). https://carpo-bonn.org/media/pages/publikationen/weitere/economic-confidence-building-measures-civil-servant-salaries/a01e701e57-1733145216/rethinking-yemens-economy-policy-brief-11.pdf (cit. on pp. 5, 216).

[16] Al Izki, F. H. S. (2019). *Exploring the organisational, social and cultural factors influencing those employee attitudes and behaviours that impact the implementation of an information security culture within Omani organisations* [Doctoral dissertation, University of Strathclyde]. https://stax.strath.ac.uk/concern/theses/9019s255m (cit. on pp. 88, 183).

[17] Alagasan, K., Alkawaz, M. H., Iqbal Hajamydeen, A., & Mohammed, M. N. (2021). A review paper on advanced attendance and monitoring systems. *2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC)*, 195–200. https://doi.org/10.1109/ICSGRC53186.2021.9515249 (cit. on p. 18).

[18] Aleksieva, V., Valchanov, H., & Huliyan, A. (2020). Implementation of smart-contract, based on Hyperledger Fabric blockchain. *2020 21st International Symposium on Electrical Apparatus & Technologies (SIELA)*, 1–4. https://ieeexplore.ieee.org/abstract/document/9167043/ (cit. on p. 128).

[19] Alghamdi, W., Salama, R., Sirija, M., Abbas, A. R., & Dilnoza, K. (2023). Secure multi-party computation for collaborative data analysis. *E3S Web of Conferences*, *399*, 04034. https://www.e3s-conferences.org/articles/e3sconf/abs/2023/36/e3sconf_iconnect2023_04034/e3sconf_iconnect2023_04034.html (cit. on p. 28).

[20] Aliyu, L. Y., & Kawugana, A. (2024). The assessment of implementation of Integrated Payroll and Personnel Information System (IPPIS) in Nigeria: Their success and failures and possible remedies (case study of selected tertiary institutions in Northeast). *International Journal of Social Sciences and Management Research*, *10*(5). https://www.iiardjournals.org/get/IJSSMR/Vol%2010.

%20No.%205%202024/THE%20ASSESSMENT%20OF%20IMPLEMENTATION%2061-73.pdf (cit. on p. 213).

[21] Alkahtani, H. K. (2018). *Raising the information security awareness level in Saudi Arabian organizations through an effective, culturally aware information security framework* [PhD Thesis]. Loughborough University. https://repository.lboro.ac.uk/articles/thesis/Raising_the_information_security_awareness_level_in_Saudi_Arabian_organizations_through_an_effective_culturally_aware_information_security_framework/9407387?file=17024693 (cit. on p. 85).

[22] Alkhalifah, A., Ng, A., Kayes, A. S. M., Chowdhury, J., Alazab, M., & Watters, P. A. (2020). A taxonomy of blockchain threats and vulnerabilities. In *Blockchain for Cybersecurity and Privacy* (pp. 3–28). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9780429324932-2/taxonomy-blockchain-threats-vulnerabilities-ayman-alkhalifah-alex-ng-kayes-jabed-chowdhury-mamoun-alazab-paul-watters (cit. on p. 29).

[23] Alm, J., Martinez-Vazquez, J., & McClellan, C. (2016). Corruption and firm tax evasion [Publisher: Elsevier]. *Journal of Economic Behavior & Organization*, *124*, 146–163. https://www.sciencedirect.com/science/article/pii/S0167268115002735?casa_token=plNe9M (cit. on p. 2).

[24] Aluko, O. (2020). IPPIS: ASUU kicks as FG sacks contract lecturers. https://punchng.com/ippis-asuu-kicks-as-fg-sacks-contract-lecturers/ (cit. on pp. 5, 23).

[25] Alyami, A., Sammon, D., Neville, K., & Mahony, C. (2020). Exploring IS security themes: A literature analysis [Publisher: Informa UK Limited]. *Journal of Decision Systems*, *29*(sup1), 425–437. https://doi.org/10.1080/12460125.2020.1848379 (cit. on p. 154).

[26] Amasiatu, C. V., & Shah, M. H. (2018). First party fraud management: Framework for the retail industry [Publisher: Emerald Publishing Limited]. *International Journal of Retail & Distribution Management*, *46*(4), 350–363. https://doi.org/10.1108/IJRDM-10-2016-0185 (cit. on p. 75).

[27] Anazodo, R. O., Okoye, J. C., & Chukwuemeka, E. E. O. (2012). Civil service reforms in Nigeria: The journey so far in service delivery. *Journal of Political Studies*, *19*(2), 1–19. https://heinonline.org/HOL/P?h=hein.journals/jlo19&i=152 (cit. on p. 213).

[28] Angel, J. J., & McCabe, D. (2015). The ethics of payments: Paper, plastic, or bitcoin? *Journal of Business Ethics*, *132*(3), 603–611. https://doi.org/10.1007/s10551-014-2354-x (cit. on p. 17).

[29] Ansel, J., & Olszewski, M. (2019). BFTree — Scaling HotStuff to millions of validators. https://blog.celo.org/bftree-scaling-hotstuff-to-millions-of-validators-7d6930ee046a?gi=12f71b957222 (cit. on p. 115).

[30] Antwi, M., Adnane, A., Ahmad, F., Hussain, R., Habib ur Rehman, M., & Kerrache, C. A. (2021). The Case of HyperLedger Fabric as a blockchain solution for healthcare applications. *Blockchain: Research and Applications*, 100012. https://doi.org/10.1016/j.bcra.2021.100012 (cit. on pp. 53, 128).

[31] Aphek, M., & Cojocaru, D. (2024). Why do they do it? A comprehensive review of the fraud triangle and the fraud diamond among fraud offenders [Publisher: Babes-Bolyai University, Educational Sciences Department]. *Educatia 21*, (28), 0_1–398. https://www.ceeol.com/search/article-detail?id=1301686 (cit. on p. 57).

[32] Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking bitcoin: Routing attacks on cryptocurrencies. *2017 IEEE symposium on security and privacy (SP)*, 375–392. https://ieeexplore.ieee.org/document/7958588/ (cit. on p. 47).

[33] Archer, B. (1979). Design as a discipline [Publisher: Elsevier]. *Design studies*, *1*(1), 17–20. https://doi.org/10.1016/0142-694X(79)90023-1 (cit. on p. 129).

[34] Arkorful, V. E., Lugu, B. K., Hammond, A., & Basiru, I. (2021). Decentralization and citizens' participation in local governance: Does trust and transparency matter? – An empirical study. *Forum for Development Studies*, *48*(2), 199–223. https://doi.org/10.1080/08039410.2021.1872698 (cit. on p. 105).

[35] Armisén, R., & Gaiatas, F. (2009, Jan.). Handbook of Hydrocolloids (Second Edition). In G. O. Phillips & P. A. Williams (Eds.), *Handbook of Hydrocolloids*

*(Second Edition)* (pp. 82–107). Woodhead Publishing. https://doi.org/10.1533/9781845695873.82 (cit. on p. 84).

[36] Arum, I., Likinyo, O. S., & Eunice, F., Olaitan. (2024). Civil Service Reforms in Nigeria. *Social Science and Humanities Journal*, *8*(11), 5735–5743. https://doi.org/10.18535/sshj.v8i11.1207 (cit. on p. 213).

[37] Ashforth, B. E., & Anand, V. (2003). The normalization of corruption in organizations [Publisher: Elsevier]. *Research in organizational behavior*, *25*, 1–52. https://doi.org/10.1016/S0191-3085(03)25001-2 (cit. on p. 59).

[38] Asif, R., & Hassan, S. R. (2023). Shaping the future of Ethereum: Exploring energy consumption in Proof-of-Work and Proof-of-Stake consensus [Publisher: Frontiers Media SA]. *Frontiers in Blockchain*, *6*, 1151724. https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2023.1151724/full (cit. on p. 35).

[39] Atmowardoyo, H. (2018). Research methods in TEFL studies: Descriptive research, case study, error analysis, and R & D. *Journal of Language Teaching and Research*, *9*(1), 197. https://doi.org/10.17507/jltr.0901.25 (cit. on pp. 83, 84, 89, 183).

[40] Awan, F., & Nunhuck, S. (2020). Governing blocks: Building interagency consensus to coordinate humanitarian aid. *Journal of Science Policy & Governance*, *16*(02), 1–27. http://www.sciencepolicyjournal.org/uploads/5/4/3/4/5434385/awan_nunhuck_jspg_v16.2.pdf (cit. on p. 54).

[41] B. Rawat, D., Chaudhary, V., & Doku, R. (2020). Blockchain technology: Emerging applications and use cases for secure and trustworthy smart systems [Publisher: MDPI]. *Journal of Cybersecurity and Privacy*, *1*(1), 4–18. https://www.mdpi.com/2624-800X/1/1/2 (cit. on p. 127).

[42] Baliga, A., Subhod, I., Kamat, P., & Chatterjee, S. (2018, July). Performance evaluation of the Quorum blockchain platform [arXiv:1809.03421 [cs]]. https://doi.org/10.48550/arXiv.1809.03421 (cit. on pp. 16, 111).

[43] Bank, W. (2023). Primary Data Collection - Dimewiki. https://dimewiki.worldbank.org/Primary_Data_Collection (cit. on p. 87).

[44] Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2019). SoK: Consensus in the age of blockchains. *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, 183–198. https://doi.org/10.1145/3318041.3355458 (cit. on p. 41).

[45] Barbosa, R. P., Martins, A. S., Da Silva, I. P. A., Costa, L. A., Oliveira, R. A., & De Souza, H. C. (2020). Acceptance and use of a virtual learning environment (VLE): Structural equations modeling of the unified theory of acceptance and use of technology. *Int J Innov Educ Res*, *8*(4), 237–244 (cit. on p. 73).

[46] BBC. (2021). Leicestershire cancer charity scammers jailed. *BBC News*. https://www.bbc.com/news/uk-england-leicestershire-58765987 (cit. on pp. 6, 168).

[47] Beardsmore, E., & McSherry, R. (2017). Healthcare workers' perceptions of organisational culture and the impact on the delivery of compassionate quality care. *Journal of Research in Nursing*, *22*(1-2), 42–56. https://doi.org/10.1177/1744987116685594 (cit. on p. 155).

[48] Beasley, M. S., Carcello, J. V., Hermanson, D. R., & Lapides, P. D. (2000). Fraudulent financial reporting: Consideration of industry traits and corporate governance mechanisms. *Accounting horizons*, *14*(4), 441–454. https://doi.org/10.2308/acch.2000.14.4.441 (cit. on pp. 153, 154).

[49] Behara, G. K., & Khandrika, T. (2020). Blockchain as a disruptive technology: Architecture, business scenarios, and future trends. In *AI and Big Data's Potential for Disruptive Innovation* (pp. 130–173). IGI Global. https://www.igi-global.com/chapter/blockchain-as-a-disruptive-technology/236338 (cit. on p. 28).

[50] Bello, M., & Mela, K. (2022). IPPIS policy and the challenges of its implementation in the Nigerian Universities: A conceptual discourse. *KIU Journal of Social Sciences, Kampala International University ISSN*, 2413–9580. Retrieved Aug. 30, 2025, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4244069 (cit. on p. 213).

[51] Bello, M. I. (2021a). Blockchain Technology and Payroll Systems. https://pureportal.strath.ac.uk/en/activities/improving-payroll-systems-in-developing-

countries-using-blockchai%20University%20of%20Strathclyde,%20Glasgow%20-%20United%20Kingdom (cit. on pp. xvii, 31).

[52] Bello, M. I. (2021b). Doctoral School Multidisciplinary Symposium 2021 - University of Strathclyde. https://pureportal.strath.ac.uk/en/activities/doctoral-school-multidisciplinary-symposium-2021-event-3 (cit. on p. xviii).

[53] Bello, M. I. (2021c). The Scottish Informatics and Computer Science Alliance (SICSA) (External organisation). https://pureportal.strath.ac.uk/en/activities/the-scottish-informatics-and-computer-science-alliance-sicsa-exte (cit. on p. xix).

[54] Bello, M. I. (2022). Doctoral School Multidisciplinary Symposium 2022 - University of Strathclyde. https://pureportal.strath.ac.uk/en/activities/strathclyde-doctoral-school-multidisciplinary-symposium-2022-even (cit. on p. xviii).

[55] Bello, M. I., & Thomas, D. R. (2022). Potentials of blockchain technology for payroll systems. *SAIS 2022 Proceedings*. https://aisel.aisnet.org/sais2022/20/ (cit. on pp. xvii, 3, 134).

[56] Bello, M. I., & Thomas, D. R. (2023). Curbing ghost worker fraud in developing countries using consortium blockchain. *Proceedings of the 9th ACM International Workshop on Security and Privacy Analytics*, 77–83. https://doi.org/10.1145/3579987.3586569 (cit. on pp. xvii, 3, 134, 214).

[57] Bello, M. I., & Thomas, D. R. (2025). Blockchain framework for enhancing employment integrity process to curb ghost worker fraud: NCSC ACE-CSR Conference 2025 (cit. on p. xvii).

[58] Belz, D. (2022). Blockchain: A cyber defense force multiplier [Publisher: Policy Studies Organization]. *Global Security & Intelligence Studies*, *7*(1), 195–202. https://gsis.scholasticahq.com/article/37629.pdf (cit. on p. 114).

[59] Besu. (2024). Public networks — Besu documentation. https://besu.hyperledger.org/public-networks (cit. on p. 109).

[60] Bhurani, K., Dogra, A., Agarwal, P., Shrivastava, P., Singh, T. P., & Bhandwal, M. (2024). Smart contracts for ensuring data integrity in cloud storage with

blockchain. *EAI Endorsed Transactions on Scalable Information Systems*. https://publications.eai.eu/index.php/sis/article/view/5633 (cit. on p. 121).

[61] Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., Song, H., Alshamari, M., & Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security [Conference Name: IEEE Access]. *IEEE Access*, *9*, 61048–61073. https://doi.org/10.1109/ACCESS.2021.3072849 (cit. on pp. 28, 33, 36).

[62] Bitpanda. (2022). What is a 51% attack and how is it prevented? https://www.bitpanda.com/academy/en/lessons/what-is-a-51-attack-and-how-is-it-prevented (cit. on p. 43).

[63] Blancaflor, E. B., Cortez, M. M. T., Geneta, D. M., Miembro, N. T. D., & Alegre, C. B. G. (2023). Comparative analysis of cybersecurity frameworks utilized by industries in the Philippines. *2023 IEEE 3rd International Conference on Computer Systems (ICCS)*, 158–162. https://doi.org/10.1109/ICCS59700.2023.10335521 (cit. on p. 158).

[64] Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for industry 4.0: A comprehensive review [Conference Name: IEEE Access]. *IEEE Access*, *8*, 79764–79800. https://doi.org/10.1109/ACCESS.2020.2988579 (cit. on p. 28).

[65] Boel, P. (2019). Payment systems – history and challenges. *Payment Systems*, 16. https://www.riksbank.se/globalassets/media/rapporter/pov/artiklar/engelska/2019/190613/er-2019_1-payment-systems--historical-evolution-and-literature-review.pdf (cit. on p. 16).

[66] Bonyuet, D. (2020). Overview and impact of blockchain on auditing. *The International Journal of Digital Accounting Research*, 31–43. https://doi.org/10.4192/1577-8517-v20_2 (cit. on p. 127).

[67] Bosunia, N. A., Prity, J. A., Jabin, J. J., Hasan, M., Rashid, M. R. A., & Tuhin, R. A. (2023). An application of decentralized product authentication system for supply chain management using blockchain technology. *2023 26th*

*International Conference on Computer and Information Technology (ICCIT)*, 1–6. https://ieeexplore.ieee.org/abstract/document/10441094/ (cit. on p. 229).

[68] Bourgeois, D. T. (2014). Information systems for business and beyond, 167. https://www.biola.edu/library/about/archives-and-special-collections (cit. on p. 31).

[69] Bowman, M., Das, D., Mandal, A., & Montgomery, H. (2021). On Elapsed Time Consensus Protocols. In A. Adhikari, R. Küsters, & B. Preneel (Eds.), *Progress in Cryptology – INDOCRYPT 2021* (pp. 559–583). Springer International Publishing. https://doi.org/10.1007/978-3-030-92518-5_25 (cit. on p. 35).

[70] Branic, N. (2015, Dec.). Routine Activities Theory. In W. G. Jennings (Ed.), *The Encyclopedia of Crime and Punishment* (1st ed., pp. 1–3). Wiley. https://doi.org/10.1002/9781118519639.wbecpx059 (cit. on p. 64).

[71] Brasel, K., Haider, A., & Haukoos, J. (2020). Practical guide to survey research [Publisher: American Medical Association]. *JAMA surgery*, *155*(4), 351–352. https://jamanetwork.com/journals/jamasurgery/article-abstract/2759264 (cit. on p. 82).

[72] Braun, J. (2015). Maintaining security and trust in large scale public key infrastructures [Publisher: Technische Universität Darmstadt]. https://tuprints.ulb.tu-darmstadt.de/4566 (cit. on p. 27).

[73] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa (cit. on pp. 154, 155).

[74] Brown, R. G., Carlyle, J., Grigg, I., & Hearn, M. (2016). Corda: An introduction. *R3 CEV, August*, *1*(15), 14 (cit. on p. 53).

[75] Budel, A., Alhabib, R., Nicholson, M., & Yadav, P. (2023, Nov.). VINCY: A Smart-contract based data integrity and validation tooling for automated vehicle incident investigation [arXiv:2311.13728 [cs]]. https://doi.org/10.48550/arXiv.2311.13728 (cit. on p. 52).

[76] Burns, W. (2017). The case for case studies in confronting environmental issues [Publisher: University of California Press, Journals & Digital Publishing Divi-

sion]. *Case Studies in the Environment*, *1*(1), 1–4. https://doi.org/10.1525/cse.2019.eic.001 (cit. on p. 148).

[77] Burns, W. (2019). The case for case studies in the context of environmental issues—updated. *Case Stud Environ*, *3*(1), 1–5. https://doi.org/10.1525/cse.2019.eic.001 (cit. on p. 148).

[78] Burra, R., Tandon, A., & Mittal, S. (2024). Empowering SMPC: Bridging the gap between scalability, memory efficiency and privacy in neural network inference. *2024 16th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, 1–6. https://ieeexplore.ieee.org/abstract/document/10427509/ (cit. on p. 28).

[79] Buscaglia, E. (2001). An analysis of judicial corruption and its causes: An objective governing-based approach. *International Review of Law and Economics*, *21*(2), 233–249. https://doi.org/10.1016/S0144-8188(01)00058-8 (cit. on p. 20).

[80] Buterin, V. (2015, Aug.). On public and private blockchains [Section: Markets]. https://www.coindesk.com/markets/2015/08/07/vitalik-buterin-on-public-and-private-blockchains/ (cit. on p. 37).

[81] Byung, P. (2018). Former UPMC claims director sentenced to prison for embezzling $846K through ghost employees. https://www.justice.gov/usao-wdpa/pr/former-upmc-claims-director-sentenced-prison-embezzling-846k-through-ghost-employees (cit. on p. 5).

[82] Cain, M., & Mittman, R. (2002). Diffusion of Innovation in healthcare. *California Health Care Foundation*. https://www.professorcarlson.net/c4dcourse/module_2/m2_unit2/m2_u2_optional/ (cit. on pp. 67, 68, 70).

[83] Caminer, D., Land, F., Aris, J., & Hermon, P. (1997). *LEO: The incredible story of the world's first business computer*. McGraw-Hill Professional. https://dl.acm.org/doi/abs/10.5555/550409 (cit. on p. 18).

[84] Capital, F. (2024). Hyperledger Besu: Unleashing the potential of ethereum in enterprises. https://fastercapital.com/content/Hyperledger-Besu--Unleashing-the-Potential-of-Ethereum-in-Enterprises.html (cit. on p. 110).

[85] Carstensen, A.-K., & Bernhard, J. (2019). Design science research – a powerful tool for improving methods in engineering education research [Publisher: Taylor & Francis _eprint: https://doi.org/10.1080/03043797.2018.1498459]. *European Journal of Engineering Education*, *44*(1-2), 85–102. https://doi.org/10.1080/03043797.2018.1498459 (cit. on p. 128).

[86] Cassez, F., Fuller, J., Ghale, M. K., Pearce, D. J., & Quiles, H. M. A. (2023, Mar.). Formal and executable semantics of the ethereum virtual machine in dafny [arXiv:2303.00152 [cs]]. https://doi.org/10.48550/arXiv.2303.00152 (cit. on p. 111).

[87] Castro, M., & Liskov, B. (1999). Practical byzantine fault tolerance [Issue: 1999]. *OsDI*, *99*, 173–186. https://www.usenix.org/legacy/publications/library/proceedings/osdi99/full_papers/castro/castro.ps (cit. on p. 108).

[88] Chamberlain, P. M., & Bowen, S. J. (2006). Designers' use of the artefact in human-centred design. In J. Clarkson, P. Langdon, & P. Robinson (Eds.), *Designing Accessible Technology* (pp. 65–74). Springer-Verlag. https://doi.org/10.1007/1-84628-365-5_7 (cit. on p. 135).

[89] Chen, F., Xiao, Z., Cui, L., Lin, Q., Li, J., & Yu, S. (2020). Blockchain for Internet of things applications: A review and open issues. *Journal of Network and Computer Applications*, *172*, 102839. https://doi.org/10.1016/j.jnca.2020.102839 (cit. on p. 53).

[90] Chen, Y., Richter, J. I., & Patel, P. C. (2021). Decentralized governance of digital platforms. *Journal of Management*, *47*(5), 1305–1337. https://doi.org/10.1177/0149206320916755 (cit. on p. 106).

[91] Chen, Y., Chen, S., Liang, J., Feagan, L. W., Han, W., Huang, S., & Wang, X. S. (2020). Decentralized data access control over consortium blockchains. *Information Systems*, *94*, 101590. https://doi.org/10.1016/j.is.2020.101590 (cit. on p. 106).

[92] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339 (cit. on pp. 31, 52, 214, 216).

[93] Chuttur, M. (2009). Overview of the technology acceptance model: Origins, developments and future directions. *Association for Information Systems AIS Electronic Library (AISeL)*. https://aisel.aisnet.org/sprouts_all/290/?utm (cit. on p. 71).

[94] Clint, B. (2020). IBM blockchain automates contract labor processes. https://www.cio.com/article/201952/ibm-blockchain-automates-contract-labor-processes.html (cit. on p. 52).

[95] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A Routine Activity approach [Publisher: [American Sociological Association, Sage Publications, Inc.]]. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589 (cit. on pp. 63, 64).

[96] Cook, P. J. (1986). The demand and supply of criminal opportunities. *Crime and Justice*, *7*, 1–27. https://doi.org/10.1086/449111 (cit. on p. 63).

[97] Corradini, F., Marcelletti, A., Morichetta, A., Polini, A., Re, B., & Tiezzi, F. (2022). Engineering trustable and auditable choreography-based systems using blockchain. *ACM Transactions on Management Information Systems*, *13*(3), 31:1–31:53. https://doi.org/10.1145/3505225 (cit. on p. 31).

[98] Cristian, N. (2019). Analysis of Fraud Triangle, Fraud Diamond and Fraud Pentagon Theory to detecting corporate fraud in Indonesia. *The International Journal of Business Management and Technology*, *3*(4) (cit. on p. 62).

[99] Crook, R. C. (2003). Decentralization and good governance [Publisher: McGill-Queen's University Press Ithaca, NY]. *Federalism in a changing world: Learning from each other*, 299–333. http://www.forumfed.org/libdocs/IntConfFed02/StG-Crook.pdf (cit. on p. 105).

[100] Cross, N. (2006). Designerly ways of knowing. In *Designerly Ways of Knowing* (pp. 1–13). Springer-Verlag. https://doi.org/10.1007/1-84628-301-9_1 (cit. on p. 129).

[101] Cryptography Introduction [Section: Computer Networks]. (2018, Nov.). https://www.geeksforgeeks.org/cryptography-introduction/ (cit. on p. 32).

[102] Cullen, F. T. (2004). Criminal Circumstance: A dynamic multicontextual criminal opportunity theory [Publisher: SAGE Publications Inc]. *Contemporary Sociology*, *33*(3), 359–361. https://doi.org/10.1177/009430610403300360 (cit. on p. 63).

[103] Dameron, M. (2018). Beigepaper: An ethereum technical specification. *Ethereum project beige paper*. https://cryptorating.eu/whitepapers/Ethereum/beigepaper.pdf (cit. on p. 111).

[104] Daniels, I. (2022, May). N80bn fraud: Arrest of Accountant-general proves IPPIS conduit, ASUU says. https://punchng.com/n80bn-fraud-arrest-of-accountant-general-proves-ippis-conduit-asuu-says/ (cit. on p. 20).

[105] Darke, P., Shanks, G., & Broadbent, M. (1998). Successfully completing case study research: Combining rigour, relevance and pragmatism [Publisher: John Wiley & Sons, Ltd]. *Information Systems Journal*, *8*(4), 273–289. https://doi.org/10.1046/j.1365-2575.1998.00040.x (cit. on p. 149).

[106] Darwish, A. N., Deepak, P., Joydeb, D., & Ernesto, D. (2023). Role-Based Access Control in private blockchain for IoT integrated smart contract. https://link.springer.com/chapter/10.1007/978-3-031-45882-8_16 (cit. on p. 126).

[107] David, E. (2024, Aug.). Police, others linked to over 22,000 suspicious entries on federal payroll. https://thesun.ng/police-others-linked-to-over-22000-suspicious-entries-on-federal-payroll/ (cit. on p. 123).

[108] Delaney, L. (2010). Descriptive statistics: Simply telling a story. *African Journal of Midwifery and Women's Health*, *4*(1), 43–48. https://doi.org/10.12968/ajmw.2010.4.1.46313 (cit. on p. 85).

[109] Demarest, L., Langer, A., & Ukiwo, U. (2020). Nigeria's Federal Character Commission (FCC): A critical appraisal [Publisher: Routledge]. *Oxford Development Studies*. https://www.tandfonline.com/doi/abs/10.1080/13600818.2020.1727427 (cit. on p. 119).

[110] Denscombe, M. (2008). Communities of practice: A research paradigm for the mixed methods approach [Publisher: SAGE Publications]. *Journal of Mixed*

*Methods Research*, *2*(3), 270–283. https://doi.org/10.1177/1558689808316807 (cit. on pp. 89, 90, 183).

[111] Deshmukh, P., Kalwaghe, S., Appa, A., & Pawar, A. (2020). Decentralised freelancing using ethereum blockchain. *2020 International Conference on Communication and Signal Processing (ICCSP)*, 881–883. https://doi.org/10.1109/ICCSP48568.2020.9182127 (cit. on p. 71).

[112] Devi, P. N. C., Widanaputra, A. A. G. P., Budiasih, I., & Rasmini, N. K. (2021). The effect of fraud Pentagon theory on financial statements: Empirical evidence from Indonesia [Publisher: Korea Distribution Science Association]. *The Journal of Asian Finance, Economics and Business*, *8*(3), 1163–1169. https://koreascience.kr/article/JAKO202106438543732.page (cit. on p. 62).

[113] Devin, K., & Shalonda, S. (2022). Purposes of research: Exploratory, descriptive and explanatory - Video and lesson transcript. https://study.com/academy/lesson/purposes-of-research-exploratory-descriptive-explanatory.html (cit. on p. 85).

[114] Diebolt, C., & Haupert, M. (Eds.). (2016). *Handbook of cliometrics*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-40406-1 (cit. on p. 16).

[115] Diffie, W., Hellman, M. E., & Ellis, J. (1976). Public key cryptography. *IEEE International Symposium on Information Theory*. https://eclass.uniwa.gr/modules/document/file.php/CSCYB105/Lectures%202020-2021/Presentation6_pk.pdf (cit. on p. 52).

[116] Dong, X., Litos, O. S. T., Tas, E. N., Tse, D., Woll, R. L., Yang, L., & Yu, M. (2025, Apr.). Remote staking with optimal economic safety [arXiv:2408.01896 [cs]]. https://doi.org/10.48550/arXiv.2408.01896 (cit. on p. 115).

[117] Doskey, T., & Stacylee, J. (2018). Blockchain technology in the department of defense. *Public Policy*, 86 (cit. on p. 54).

[118] Doudou, A., Garbinato, B., & Guerraoui, R. (2000). Abstractions for devising Byzantine-resilient state machine replication. *Proceedings 19th IEEE Symposium on Reliable Distributed Systems SRDS-2000*, 144–153. https://doi.org/10.1109/RELDI.2000.885402 (cit. on p. 115).

[119] Druschel, P. (2008). Accountability for distributed systems. *Proceedings of the twenty-seventh ACM symposium on Principles of distributed computing*, 13–14. https://doi.org/10.1145/1400751.1400754 (cit. on p. 218).

[120] Dubai Land Department - Annual report: Real estate sector performance 2019. (2019). https://dubailand.gov.ae/en/ (cit. on p. 53).

[121] Duong, K. (2022). Research Guides: Qualtrics: What is Qualtrics? https://csulb.libguides.com/qualtrics/about (cit. on pp. 93, 190).

[122] EACC. (2024). https://eacc.go.ke/en/default (cit. on p. 166).

[123] Eden, C., & Ackermann, F. (1998). *Making strategy: The journey of strategic management*. Sage. (Cit. on p. 119).

[124] Editorial. (2021, Jan.). The ghost workers syndrome in Nigeria. https://www.vanguardngr.com/2021/01/the-ghost-workers-syndrome-in-nigeria/ (cit. on p. 216).

[125] EFCC, E. (2017). Economic and Financial Crimes Commission - EFCC - N11m Fraud: Court begins trial within trial of "ghost worker". https://www.efcc.gov.ng/efcc/news-and-information/news-release/2764-n11m-fraud-court-begins-trial-within-trial-of-ghost-worker (cit. on pp. 6, 163).

[126] Efosa, T. (2024, June). How we cracked down on ghost workers abroad earning salaries in civil service. https://www.vanguardngr.com/2024/06/how-we-cracked-down-on-ghost-workers-abroad-earning-salaries-in-civil-service-yemi-esan/ (cit. on p. 176).

[127] Eisenberg, E., & Gale, D. (1959). Consensus of subjective probabilities: The Pari-Mutuel method [Publisher: Institute of Mathematical Statistics]. *The Annals of Mathematical Statistics*, *30*(1), 165–168. https://www.jstor.org/stable/2237130 (cit. on p. 41).

[128] Ekiti Election. (2022, June). Ekiti election: UK decries vote buying [Section: Politics]. https://www.sunnewsonline.com/ekiti-election-uk-decries-vote-buying/ (cit. on p. 22).

[129] Ekparinya, P., Gramoli, V., & Jourjon, G. (2019, Sept.). The Attack of the clones against Proof-of-Authority [arXiv:1902.10244 [cs]]. https://doi.org/10.48550/arXiv.1902.10244 (cit. on p. 115).

[130] Emanghe, E. E., & Amoramo, J. D. (2020). Integrated Payroll and Personnel Information System (IPPIS) for sustainability of university education in Nigeria after COVID-19 pandemic [Number: 1]. *International Journal of Capacity Building in Education and Management*, *4*(1), 35–43. http://journals.rcmss.com/index.php/ijcbem/article/view/55 (cit. on p. 23).

[131] Engelmann, C., Scott, S. L., Leangsuksun, C., & He, X. (2007). Transparent symmetric active/active replication for service-level high availability. *Seventh IEEE International Symposium on Cluster Computing and the Grid (CCGrid '07)*, 755–760. https://doi.org/10.1109/CCGRID.2007.116 (cit. on p. 114).

[132] Evenstad, L. (2016). DWP trials blockchain technology for benefit payments. https://www.computerweekly.com/news/450300034/DWP-trials-blockchain-technology-for-benefit-payments (cit. on pp. 29, 54).

[133] Faguet, J.-P. (2014). Decentralization and governance. *World Development*, *53*, 2–13. https://doi.org/10.1016/j.worlddev.2013.01.002 (cit. on p. 105).

[134] Fan, C., Lin, C., Khazaei, H., & Musilek, P. (2022). Performance analysis of hyperledger besu in private blockchain. *2022 IEEE international conference on decentralized applications and infrastructures (DAPPS)*, 64–73. https://ieeexplore.ieee.org/abstract/document/9899854/ (cit. on pp. 113, 114).

[135] Felson, M. (2017). Routine activities and crime prevention in the developing metropolis. In *Crime Opportunity Theories* (pp. 91–111). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315095301-5/routine-activities-crime-prevention-developing-metropolis-marcus-felson (cit. on p. 64).

[136] Ferreira, A. I. M. (1995). El humanismo médico en la Universidad de Alcalá: Siglo XVI. https://philpapers.org/rec/FEREHM-2 (cit. on p. 17).

[137] Fleming, S. (2019). Corruption costs developing countries $1.26 trillion every year - yet half of EMEA think it's acceptable. https://www.weforum.org/agenda/2019/12/corruption-global-problem-statistics-cost/ (cit. on p. 19).

[138] Folorunso, O. (2022). The Integrated Payroll and Personnel Information Systems (IPPIS) and public service salary administration in Nigeria. *International Journal of Research and Innovation in Social Science (IJRISS)*, *6*, 578–586. https://doi.org/10.47772/IJRISS.2022.6436 (cit. on pp. 89, 183).

[139] Forbes. (2024, June). Cryptocurrency prices, market cap and charts. https://www.forbes.com/digital-assets/crypto-prices/,%20https://www.forbes.com/digital-assets/crypto-prices/ (cit. on p. 29).

[140] França, F. A., J., A. N. J., Gonçalves, G. R., & Almeida, A. (2020). Proposing the use of blockchain to improve the solid waste management in small municipalities. *Journal of Cleaner Production*, *244*, 118529. https://doi.org/10.1016/j.jclepro.2019.118529 (cit. on p. 106).

[141] Fraser, J. R., Simkins, B., & Narvaez, K. (2014). *Implementing enterprise risk management: Case studies and best practices*. John Wiley & Sons. https://www.semanticscholar.org/paper/Implementing-Enterprise-Risk-Management%3A-Case-and-Fraser-Simkins/ (cit. on p. 153).

[142] Freeze, R. D., Alshare, K. A., Lane, P. L., & Wen, H. J. (2010). IS success model in e-learning context based on students' perceptions. *Journal of Information systems education*, *21*(2), 173–184 (cit. on pp. 76, 77).

[143] Furidha, B. W. (2023). Comprehension of the descriptive qualitative research method: A critical assessment of the literature. *Acitya Wisesa: Journal Of Multidisciplinary Research*, 1–8. https://www.journal.jfpublisher.com/index.php/jmr/article/view/443 (cit. on p. 85).

[144] Gabriel, O. (2019). Government Integrated Financial Management Information System (GIFMIS) as a tool for effective management of government finances. https://www.academia.edu/40075507/government_integrated_financial_management_information_system_gifmis_as_a_tool_for_effective_management_of_government_finances (cit. on p. 2).

[145] Garay, J., Kiayias, A., & Leonardos, N. (2024). The bitcoin backbone protocol: Analysis and applications. *J. ACM*, *71*(4), 25:1–25:49. https://doi.org/10.1145/3653445 (cit. on p. 114).

[146] Gavin, W. (2015). Ethereum Guide. https://github.com/ethereum/guide/blob/master/poa.md (cit. on p. 109).

[147] Genevieve, O., Ifeoma, N., Aniel, K., & Ehisuoria, A. (2025). The role of forensic auditing in strengthening corporate transparency and fraud prevention in financial institutions. *Finance & Accounting*, *7*(2), 126–132. https://elibrary.ru/item.asp?id=82063491 (cit. on p. 65).

[148] George, T., & Merkus, J. (2022). Explanatory research — Definition, guide, and examples. https://www.scribbr.com/methodology/explanatory-research/ (cit. on p. 86).

[149] Giri, G., Chakate, K., Gonge, S., Joshi, R., Kotecha, K., Mishra, O., Parashar, D., & Mulay, P. (2023). Payroll management using blockchain. In A. E. Hassanien, O. Castillo, S. Anand, & A. Jaiswal (Eds.), *International Conference on Innovative Computing and Communications* (pp. 369–377). Springer Nature. https://doi.org/10.1007/978-981-99-3315-0_28 (cit. on p. 40).

[150] Glaser, V. L., Fast, N. J., Harmon, D. J., & Green Jr, S. E. (2016). Institutional frame switching: How institutional logics shape individual action. In *How institutions matter!* (pp. 35–69). Emerald Group Publishing Limited. https://www.emerald.com/insight/content/doi/10.1108/S0733-558X201600048A001/full/html (cit. on p. 66).

[151] Glicken, M. D. (2003). *Social research: A simple guide*. Pearson College Division. (Cit. on p. 86).

[152] Goel, R. K., & Saunoris, J. W. (2016). Government Decentralization and Prevalence of the Shadow Economy. *Public Finance Review*, *44*(2), 263–288. https://doi.org/10.1177/1091142114545677 (cit. on pp. 216, 217).

[153] Goh, E., & Sigala, M. (2020). Integrating Information & Communication Technologies (ICT) into classroom instruction: Teaching tips for hospitality educators from a diffusion of innovation approach. *Journal of Teaching in Travel & Tourism*, *20*(2), 156–165. https://doi.org/10.1080/15313220.2020.1740636 (cit. on p. 69).

[154] Gomberg-Muñoz, R. M. (2018). Review essay: Law and migrant labor in the 20th century: Ghost workers and global capitalism. https://ecommons.luc.edu/anthropology_facpubs/21/ (cit. on p. 38).

[155] Gosling, S. D., Vazire, S., Srivastava, S., & John, O. P. (2004). Should we trust web-based studies? A comparative analysis of six preconceptions about internet questionnaires [Place: US Publisher: American Psychological Association]. *American Psychologist*, *59*(2), 93–104. https://doi.org/10.1037/0003-066X.59.2.93 (cit. on p. 87).

[156] Griffiths, C. (2004). *The case of the hybrid umbrella: A study of case studies*. Auckland Institute of Studies. Centre for Research in International Education. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=a5c420b7d712bc0b3af3fdd45f3ea1f3460bc847 (cit. on pp. 148, 149).

[157] Grover, P., Kar, A. K., & Janssen, M. (2019). Diffusion of blockchain technology: Insights from academic literature and social media analytics [Publisher: Emerald Publishing Limited]. *Journal of Enterprise Information Management*, *32*(5), 735–757. https://www.emerald.com/insight/content/doi/10.1108/JEIM-06-2018-0132/full/html (cit. on p. 69).

[158] Grover, S. (2010). Implicit informal qualitative research processes embedded in legal proceedings: A case example. *Journal of the Canadian Academy of Child and Adolescent Psychiatry*, *19*(1), 26–31. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2809443/ (cit. on p. 153).

[159] Gugnani, P., Dhakad, R. S., Sadhya, D., & Godfrey, W. W. (2025). Revisiting Proof of Stake with reward and penalty mechanism [ISSN: 2155-2509]. *2025 17th International Conference on COMmunication Systems and NETworks (COMSNETS)*, 1287–1292. https://doi.org/10.1109/COMSNETS63942.2025.10885605 (cit. on p. 116).

[160] Gupta, S., Rahnama, S., Hellings, J., & Sadoghi, M. (2020). ResilientDB: Global scale resilient blockchain fabric [arXiv:2002.00160 [cs]]. *Proceedings of the VLDB Endowment*, *13*(6), 868–883. https://doi.org/10.14778/3380750.3380757 (cit. on p. 115).

[161] Gutlapalli, S. S. (2016). Commercial applications of blockchain and distributed ledger technology. *Engineering International*, *4*(2), 89–94. https://pdfs.semanticscholar.org/91a7/7f5acd9449159693f3fde888e7fcc826406d.pdf (cit. on p. 124).

[162] Ha, Y.-H., & Kumar, S. S. (2021). Investigating decentralized renewable energy systems under different governance approaches in Nepal and Indonesia: How does governance fail? [Publisher: Elsevier]. *Energy Research & Social Science*, *80*, 102214. https://doi.org/10.1016/j.erss.2021.102214 (cit. on p. 106).

[163] Hair, J., Black, W., Babin, B., & Anderson, R. (2010). Multivariate data analysis: A Global Perspective. *7th edn (Uppersaddle River, NJ: Pearson Prentice Hall)* (cit. on pp. 90, 189).

[164] Hancock, M., & Ed, V. (2016). Distributed ledger technology: Beyond block chain. Retrieved Dec. 5, 2020, from https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain (cit. on p. 30).

[165] Hardy, J., Bell, P., & Allan, D. (2020). A crime script analysis of the Madoff Investment Scheme. *Crime Prevention and Community Safety*, *22*(1), 68–97. https://doi.org/10.1057/s41300-019-00082-6 (cit. on p. 158).

[166] Hascika, D. P., Sinurat, D. P., Dewi, A. V., Sunaryo, D., & Wulandari, S. S. (2024). Fraud factor analysis hexagon in detecting financial report fraud in listed companies in Indonesia: A systematic literature approach. *Indo-Fintech Intellectuals: Journal of Economics and Business*, *4*(5), 2589–2605 (cit. on p. 63).

[167] Hatin, J., & André, V. (2023). Decentralized Ethereum-Based solution for mitigating oracle single point of failure. *2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 1–4. https://ieeexplore.ieee.org/abstract/document/10316772/ (cit. on p. 140).

[168] Hawley, I. (2015). Ghost workers: Who are they and how to deal with them. https://www.abyrint.com/ghost-worker-stories/ (cit. on p. 4).

[169] Hechanova, M. R. M., Melgar, I., Falguera, P. Z., & Villaverde, M. (2014). Organisational culture and workplace corruption in government hospitals [Publisher: SAGE Publications]. *Journal of Pacific Rim Psychology*, *8*(2), 62–70. https://doi.org/10.1017/prp.2014.5 (cit. on p. 59).

[170] Helms, K. (2018). Venezuela makes Petro Crypto a national currency, publishes new whitepaper – Bitcoin News. https://news.bitcoin.com/venezuela-petro-new-whitepaper/ (cit. on p. 54).

[171] Herlihy, M., & Moir, M. (2016, June). Enhancing accountability and trust in distributed ledgers [arXiv:1606.07490 [cs]]. https://doi.org/10.48550/arXiv.1606.07490 (cit. on p. 31).

[172] Hildenbrandt, E., Saxena, M., Rodrigues, N., Zhu, X., Daian, P., Guth, D., Moore, B., Park, D., Zhang, Y., & Stefanescu, A. (2018). Kevm: A complete formal semantics of the ethereum virtual machine. *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, 204–217. https://ieeexplore.ieee.org/abstract/document/8429306/ (cit. on p. 111).

[173] Hollis, M. E., Felson, M., & Welsh, B. C. (2013). The capable guardian in routine activities theory: A theoretical and conceptual reappraisal [Publisher: Springer]. *Crime Prevention and Community Safety*, *15*, 65–79. https://idp.springer.com/authorize/casa?redirect_uri=https://link.springer.com/article/10.1057/cpcs.2012 (cit. on p. 64).

[174] Honar Pajooh, H., Rashid, M., Alam, F., & Demidenko, S. (2021). Hyperledger Fabric blockchain for securing the edge Internet of Things [Number: 2 Publisher: Multidisciplinary Digital Publishing Institute]. *Sensors*, *21*(2), 359. https://doi.org/10.3390/s21020359 (cit. on p. 128).

[175] Hong, B., Ly, M., & Lin, H. (2023). Robotic process automation risk management: Points to consider [Publisher: American Accounting Association]. *Journal of emerging technologies in accounting*, *20*(1), 125–145. https://publications.aaahq.org/jeta/article/20/1/125/10123 (cit. on p. 27).

[176] Hossain, S., Saha, S., Akhi, J. F., & Helaly, T. (2020). Automated tax return verification with blockchain technology [Series Title: Algorithms for Intelligent Systems]. In *Proceedings of International Joint Conference on Computational Intelligence* (pp. 45–55). Springer Singapore. https://doi.org/10.1007/978-981-15-3607-6_4 (cit. on pp. 39, 40).

[177] Howard, P., & Kris, B. (2020). Certified Blockchain Security Professional. *Blockchain Training Alliance, Inc*, *1* (cit. on pp. 42–50).

[178] Hughes, D. (2018). What is an eclipse attack? https://www.radixdlt.com/post/what-is-an-eclipse-attack (cit. on p. 45).

[179] Hurlburt, G. (2016). Might the blockchain outlive bitcoin? [Conference Name: IT Professional]. *IT Professional*, *18*(2), 12–16. https://doi.org/10.1109/MITP.2016.21 (cit. on p. 34).

[180] Hur-Yagba, A. A. (2021). Impact of recruitment and selection process on the performance of public enterprises. A study of the Nigeria Railway Corporation. [Number: 1]. *East African Journal of Business and Economics*, *3*(1), 82–97. https://doi.org/10.37284/eajbe.3.1.322 (cit. on pp. 89, 183).

[181] Hussmann, K. (2011). Addressing corruption in the health sector: Securing equitable access to health care for everyone. *U4 Issue*, *2011:1*. https://www.cmi.no/publications/3934-addressing-corruption-in-the-health-sector (cit. on p. 4).

[182] Hyperledger, C. (2024). Getting Started. https://hyperledger.github.io/caliper/v0.6.0/getting-started/ (cit. on p. 114).

[183] ICPC. (2021, Jan.). ICPC corruption verdict unsettles judiciary. https://guardian.ng/features/law/icpc-corruption-verdict-unsettles-judiciary/ (cit. on pp. 20, 22).

[184] Idowu, I. (2022, May). UPDATED: EFCC finally arrests Rochas Okorocha. https://dailytrust.com/updated-efcc-officials-arrest-rochas-okorocha (cit. on p. 20).

[185] Ilias, A., Baidi, N., Ghani, E. K., Mohammad, K., & Omonov, A. (2024). Examining government officials' perceived risk management and internal control in combating fraud in the public sector. *Edelweiss Applied Science and Technology*, *8*(3), 125–144. https://doi.org/10.55214/25768484.v8i3.804 (cit. on p. 125).

[186] Imbugwa, G. B., & Mazzara, M. (2021). Towards a secure smart parking solution for business entities. In L. Barolli, I. Woungang, & T. Enokido (Eds.), *Advanced Information Networking and Applications* (pp. 469–478). Springer International Publishing. https://doi.org/10.1007/978-3-030-75078-7_47 (cit. on p. 111).

[187] Intention-Based Models: The Theory of Planned Behavior Within the Context of IS [ISSN: 1571-0270]. (2012). In *Integrated Series in Information Systems* (pp. 219–239). Springer New York. https://doi.org/10.1007/978-1-4419-9707-4_12 (cit. on p. 73).

[188] International, T. (2021). 2021 Corruption Perceptions Index - Explore the results. https://www.transparency.org/en/cpi/2021 (cit. on pp. 20, 21).

[189] Islam, M. M., Merlec, M. M., & In, H. P. (2022). A comparative analysis of Proof-of-Authority consensus algorithms: Aura vs Clique [ISSN: 2474-2473]. *2022 IEEE International Conference on Services Computing (SCC)*, 327–332. https://doi.org/10.1109/SCC55611.2022.00054 (cit. on p. 113).

[190] Jaffer, S. A., Pandey, S., Mehta, R., & Bhavathankar, P. (2020). Blockchain based direct benefit transfer system for subsidy delivery. *2020 international conference for emerging technology (INCET)*, 1–6. https://ieeexplore.ieee.org/abstract/document/9154178/ (cit. on p. 54).

[191] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition [Publisher: IEEE]. *IEEE Transactions on circuits and systems for video technology*, *14*(1), 4–20. https://ieeexplore.ieee.org/abstract/document/1262027/ (cit. on p. 27).

[192] Jaiswal, H., Muddukrishna, B. S., & Kulyadi, G. P. (2020). Data integrity violations: A challenge to the pharmaceutical industry. *International Journal of Pharmaceutical Quality Assurance*, *11*(1), 196. https://doi.org/10.25258/ijpqa.11.1.30 (cit. on p. 118).

[193] Jaiyeola, T. (2024, Sept.). Talent gap threatens Nigeria's blockchain industry. https://businessday.ng/news/article/talent-gap-threatens-nigerias-blockchain-industry/ (cit. on p. 213).

[194] Joe, D., & Kankpang, K. (2012). Effect of fraud risk reduction strategy on the level of employee fraud in Nigerian public service organizations [Publisher: Scientia Socialis Ltd.]. *Problems of Management in the 21st Century*, *4*, 30. https://www.ceeol.com/search/article-detail?id=1034397 (cit. on p. 157).

[195] Johnson, P., & Clark, M. (2006). Mapping the terrain: An overview of business and management research methodologies. *Business and management research methodologies. London: Sage* (cit. on p. 85).

[196] Jokonya, O. (2017). Critical literature review of theory of planned behavior in the information systems research. *DEStech Transactions on Computer Science and Engineering*, (ameit). https://doi.org/10.12783/dtcse/ameit2017/12297 (cit. on pp. 73, 74).

[197] Joshi, A., Han, M., & Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing*, *1*, 121–147. https://doi.org/10.3934/mfc.2018007 (cit. on pp. 35, 36).

[198] Junger, M., Wang, V., & Schlömer, M. (2020). Fraud against businesses both online and offline: Crime scripts, business characteristics, efforts, and benefits. *Crime Science*, *9*(1), 13. https://doi.org/10.1186/s40163-020-00119-4 (cit. on pp. 158, 159).

[199] Kaminski, J. (2011). Diffusion of innovation theory. *Canadian Journal of Nursing Informatics*, *6*(2), 1–6. https://cjni.net/journal/?p=1444 (cit. on p. 67).

[200] Kassab, M. H., DeFranco, J., Malas, T., Laplante, P., destefanis giuseppe, g., & Graciano Neto, V. V. (2019). Exploring research in blockchain for healthcare and a roadmap for the future. *IEEE Transactions on Emerging Topics in Computing*, 1–1. https://doi.org/10.1109/TETC.2019.2936881 (cit. on p. 29).

[201] Kassem, R. (2012). Financial reporting fraud: Are standards' setters and external auditors doing enough? *3*(19). https://ijbssnet.com/journals/Vol_3_No_19_October_2012/32.pdf (cit. on p. 58).

[202] Katrin, V., & Liina, S. (2014). The use of the National blockchain infrastructure to support the E-residency initiative in Estonia. https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/use-national-blockchain-infrastructure-support-e-residency-initiative-estonia (cit. on p. 51).

[203] Katz, E. (1957). The two-step flow of communication: An up-to-date report on an hypothesis. *Public Opinion Quarterly*, *21*(1), 61–78. https://doi.org/10.1086/266687 (cit. on p. 67).

[204] Kaushik, A., Choudhary, A., Ektare, C., Thomas, D., & Akram, S. (2017). Blockchain — Literature survey. *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2145–2148. https://doi.org/10.1109/RTEICT.2017.8256979 (cit. on p. 32).

[205] Kennedy, L. W., & Baron, S. W. (1993). Routine activities and a subculture of violence: A Study of violence on the street. *Journal of Research in Crime and Delinquency*, *30*(1), 88–112. https://doi.org/10.1177/0022427893030001006 (cit. on p. 64).

[206] King, W. R., & He, J. (2006). A meta-analysis of the technology acceptance model [Publisher: Elsevier]. *Information & management*, *43*(6), 740–755. https://www.sciencedirect.com/science/article/pii/S0378720606000528 (cit. on p. 71).

[207] Kiriakidis, S. (2015). Theory of planned behaviour: The intention-behaviour relationship and the perceived behavioural control (PBC) relationship with intention and behaviour. *International Journal of Strategic Innovative Marketing*, *3*(2), 40–51 (cit. on p. 73).

[208] Kniepmann, C. (2020, Aug.). Fraud Triangle — Fraud Opportunity — St Louis CPA Firm. https://anderscpa.com/the-fraud-triangle-three-conditions-that-increase-the-risk-of-fraud/ (cit. on p. 57).

[209] Kohler, J. C. (2020). Findings from a rapid review of literature on ghost workers in the health sector: Towards improving detection and prevention [Accepted: 2021-10-29T13:57:21Z]. https://tspace.library.utoronto.ca/handle/1807/107933 (cit. on p. 57).

[210] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts [ISSN: 2375-1207]. *2016 IEEE Symposium on Security and Privacy (SP)*, 839–858. https://doi.org/10.1109/SP.2016.55 (cit. on p. 34).

[211] Kuhn, M., Funk, F., Zhang, G., & Franke, J. (2021). Blockchain-based application for the traceability of complex assembly structures. *Journal of Manufactur-*

*ing Systems*, *59*, 617–630. https://doi.org/10.1016/j.jmsy.2021.04.013 (cit. on pp. 52, 53).

[212] Kunhibava, S., Muneeza, A., Mustapha, Z., Karim, M. E., & Sa'ad, A. A. (2024). Selected issues in the use of RegTech in the Islamic and conventional financial markets [Publisher: Emerald Publishing Limited]. *Journal of Islamic Accounting and Business Research*, *15*(5), 746–761. https://www.emerald.com/insight/content/doi/10.1108/JIABR-03-2022-0069/full/html (cit. on p. 153).

[213] Kunle, S. (2022, May). Accountant-General of the Federation, Ahmed Idris, arrested - Premium Times Nigeria. https://www.premiumtimesng.com/news/headlines/530277-breaking-accountant-general-of-the-federation-ahmed-idris-arrested.html (cit. on p. 20).

[214] Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association : JAMIA*, *24*(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068 (cit. on p. 54).

[215] Ladage, K. ( (2021). Blockchain: Increasing efficiency and transparency across the supply chain. https://www.pharmasalmanac.com/articles/blockchain-increasing-efficiency-and-transparency (cit. on p. 30).

[216] Lallai, G., Pinna, A., Marchesi, M., & Tonelli, R. (2020). Software engineering for DApp smart contracts managing workers contracts. *DLT@ ITASEC*. https://ceur-ws.org/Vol-2580/DLT_2020_paper_8.pdf (cit. on p. 51).

[217] Lamport, L., Shostak, R., & Pease, M. (2019, Oct.). The Byzantine generals problem. In *Concurrency: The Works of Leslie Lamport*. Association for Computing Machinery. https://doi.org/10.1145/3335772.3335936 (cit. on p. 41).

[218] Lamriji, Y., Makkaoui, K. E., & Beni-Hssane, A. (2022). Towards fast ECC signing algorithms for Blockchain. *2022 5th International Conference on Networking, Information Systems and Security: Envisage Intelligent Systems in 5g//6G-based Interconnected Digital Worlds (NISS)*, 1–6. https://doi.org/10.1109/NISS55057.2022.10085497 (cit. on p. 114).

[219] Leclerc, B., & Morgenthaler, E. (2023). Examining emerging fraud facilitated by the internet through crime scripts [Publisher: Australian Institute of Criminology Woden, ACT]. *Trends and Issues in Crime and Criminal Justice*, (680), 1–28. https://search.informit.org/doi/abs/10.3316/informit.459533616387170 (cit. on p. 159).

[220] Lee, S., Kim, D., Kim, D., Son, S., & Kim, Y. (2019). Who spent my EOS? On the ({In) Security} of resource management of {EOS. IO}. *13th USENIX workshop on offensive technologies (WOOT 19)*. https://www.usenix.org/conference/woot19/presentation/lee (cit. on p. 48).

[221] Lee, Y., Kozar, K. A., & Larsen, K. R. T. (2003). The technology acceptance model: Past, present, and future. *Communications of the Association for Information Systems*, *12*, 31. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=3217&context=cais (cit. on pp. 70, 71).

[222] Leonardos, S., Reijsbergen, D., & Piliouras, G. (2020). Weighted voting on the blockchain: Improving consensus in proof of stake protocols. *International Journal of Network Management*, *30*(5), e2093. https://doi.org/10.1002/nem.2093 (cit. on p. 114).

[223] Les, L. (2013, June). Ghost workers and indulgent exorcists. https://www.vanguardngr.com/2013/06/ghost-workers-and-indulgent-exorcists/ (cit. on p. 1).

[224] Lewis, M., & Pettersson, G. (2009, Oct.). *Governance in healthcare delivery : Raising performance*. The World Bank. https://doi.org/10.1596/1813-9450-5074 (cit. on pp. 58, 59).

[225] Li, J., & Mazieres, D. (2007). Beyond one-third faulty replicas in Byzantine Fault Tolerant systems. *NSDI*, 10–10. https://www.usenix.org/legacy/events/nsdi07/tech/full_papers/li/li.pdf (cit. on p. 115).

[226] Lim, H. W., Kerschbaum, F., & Wang, H. (2012). Workflow signatures for business process compliance. *IEEE Transactions on Dependable and Secure Computing*, *9*(5), 756–769. https://doi.org/10.1109/TDSC.2012.38 (cit. on p. 52).

[227] Lim, M. K., Li, Y., Wang, C., & Tseng, M.-L. (2021). A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries. *Computers & Industrial Engineering*, *154*, 107133. https://doi.org/10.1016/j.cie.2021.107133 (cit. on p. 28).

[228] Lin, I.-C., & Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.*, *19*(5), 653–659 (cit. on pp. 37, 38).

[229] Lincke, S., & Green, D. (2012). Combating IS fraud: A teaching case study (cit. on p. 149).

[230] Lino, A. F., Azevedo, R. R. d., Aquino, A. C. B. d., & Steccolini, I. (2022). Fighting or supporting corruption? The role of public sector audit organizations in Brazil. *Critical Perspectives on Accounting*, *83*, 102384. https://doi.org/10.1016/j.cpa.2021.102384 (cit. on p. 19).

[231] Lockitch, J., Rayment-McHugh, S., & McKillop, N. (2022). Why Didn't They Intervene? Examining the Role of Guardianship in Preventing Institutional Child Sexual Abuse [Publisher: Routledge _eprint: https://doi.org/10.1080/10538712.2022.2133042]. *Journal of Child Sexual Abuse*, *31*(6), 649–671. https://doi.org/10.1080/10538712.2022.2133042 (cit. on p. 64).

[232] Lu, Q., & Xu, X. (2017). Adaptable blockchain-based systems: A case study for product traceability [Publisher: IEEE]. *Ieee Software*, *34*(6), 21–27. https://ieeexplore.ieee.org/abstract/document/8106871/ (cit. on p. 127).

[233] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016). A secure sharding protocol for open blockchains. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 17–30. https://doi.org/10.1145/2976749.2978389 (cit. on p. 52).

[234] Lyu, Q., Qi, Y., Zhang, X., Liu, H., Wang, Q., & Zheng, N. (2020). SBAC: A secure blockchain-based access control framework for information-centric networking. *Journal of Network and Computer Applications*, *149*, 102444. https://doi.org/10.1016/j.jnca.2019.102444 (cit. on p. 53).

[235] Ma, J., Jo, Y., & Park, C. (2020). PeerBFT: Making Hyperledger Fabric's ordering service withstand byzantine faults. *IEEE Access*, *8*, 217255–217267. https://doi.org/10.1109/ACCESS.2020.3040443 (cit. on p. 115).

[236] Machen, S. (2023). Thematic reviews of patient safety incidents as a tool for systems thinking: A quality improvement report [Publisher: British Medical Journal Publishing Group]. *BMJ Open Quality*, *12*(2), e002020. https://bmjopenquality.bmj.com/content/12/2/e002020.abstract (cit. on p. 155).

[237] Mahamud, S., & Alvi, S. T. (2022). A framework for Covid-19 vaccine management system using blockchain technology. *2021 4th International Conference on Recent Trends in Computer Science and Technology (ICRTCST)*, 417–422. https://doi.org/10.1109/ICRTCST54752.2022.9781924 (cit. on p. 128).

[238] Masaiti, G. (2013). Students' perceptions of financing public universities in Zambia: Toward a more sustainable and inclusive policy strategy. In *Funding Higher Education in Sub-Saharan Africa* (pp. 296–326). Palgrave Macmillan UK. http://link.springer.com/10.1057/9781137345783_12 (cit. on p. 18).

[239] Masele, J. J., & Kagoma, R. S. (2021). Usefulness of human capital management information systems on payroll reliability among public universities in Tanzania. *Public Money & Management*, *0*(0), 1–9. https://doi.org/10.1080/09540962.2021.1906579 (cit. on pp. 23, 216).

[240] Masood, F., & Faridi, A. R. (2024). Developing a novel blockchain-based vaccine tracking and certificate system: An end-to-end approach. *Peer-to-Peer Networking and Applications*. https://doi.org/10.1007/s12083-024-01662-6 (cit. on p. 128).

[241] McCombes, S. (2021, June). What is a research design — Types, guide and examples. https://www.scribbr.com/methodology/research-design/ (cit. on p. 84).

[242] Medha, B. (2016, June). Singapore Government builds blockchain system to protect banks. https://govinsider.asia/smart-gov/singapore-government-builds-blockchain-system-to-protect-banks/ (cit. on p. 54).

[243] Memon, R. A., Li, J. P., & Ahmed, J. (2019). Simulation model for blockchain systems using queuing theory [Number: 2 Publisher: Multidisciplinary Digital Publishing Institute]. *Electronics*, *8*(2), 234. https://doi.org/10.3390/electronics8020234 (cit. on p. 128).

[244] Mendis, G. J., Wu, Y., Wei, J., Sabounchi, M., & Roche, R. (2020). A blockchain-powered decentralized and secure computing paradigm [Publisher: IEEE]. *IEEE Transactions on Emerging Topics in Computing*, *9*(4), 2201–2222. https://ieeexplore.ieee.org/abstract/document/9050459/ (cit. on p. 32).

[245] Merriam-Webster. (1997). *Merriam-Webster's collegiate dictionary* (10th ed.) [Open Library ID: OL1003185M]. (Cit. on p. 75).

[246] Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, *83*(2), 340–363. https://doi.org/10.1086/226550 (cit. on p. 66).

[247] Micah, L. C., & Moses, T. (2018). IPPIS and the ghost workers' syndrome in Nigeria's public sector. *SAS Publishers (Scholars Academic and Scientific Publishers)*, *5*(8), 773–778. https://doi.org/10.21276/sjebm.2018.5.8.8 (cit. on pp. 1, 5, 214, 216).

[248] Michael, B. (2022). Airport cleaning contractor pleads to fraud, money laundering in 'ghost' worker scam. https://www.news-press.com/story/news/2022/04/04/fort-myers-airport-contractor-guilty-900-k-ghost-worker-scam-rsw-thomas-brennan/7271061001/ (cit. on p. 173).

[249] Min, S., So, K., & Jeong, M. (2021). Consumer adoption of the Uber mobile application: Insights from diffusion of innovation theory and technology acceptance model. In *Future of tourism marketing* (pp. 2–15). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003176039-2/consumer-adoption-uber-mobile-application-insights-diffusion-innovation-theory-technology-acceptance-model-somang-min-kevin-kam-fung-miyoung-jeong (cit. on p. 69).

[250] Mishra, A., & Raghatate, K. S. (2025). Blockchain for safe credential checking in hiring. *2025 International Conference on Intelligent Control, Computing*

*and Communications (IC3)*, 1006–1012. https://ieeexplore.ieee.org/abstract/document/10957402/ (cit. on p. 55).

[251] Mishra, S. B., & Alok, S. (2022). *Handbook of research methodology*. Educreation publishing. https://dspace.unitywomenscollege.ac.in/bitstream/123456789/1319/1/BookResearchMethodology.pdf (cit. on p. 82).

[252] Misrak, M., & Kate, T. (2016, Sept.). Six reasons ministries of finance should invest in health workers. https://www.intrahealth.org/vital/six-reasons-ministries-finance-should-invest-health-workers (cit. on pp. 5, 216).

[253] Mitcham, C. (2022). *Thinking through technology: The path between engineering and philosophy*. Teorema: Revista Internacional de Filosofía. https://www.jstor.org/stable/43047305 (cit. on p. 128).

[254] Mitchell, M. L., & Jolley, J. M. (2013). *Research design explained* (Eighth edition, International edition) [OCLC: 942680909]. Wadsworth Cengage Learning. http://www.dawsonera.com/depp/reader/protected/external/AbstractView/S9781473702950 (cit. on p. 87).

[255] Miyachi, K., & Mackey, T. K. (2021). hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Information Processing & Management*, *58*(3), 102535. https://doi.org/10.1016/j.ipm.2021.102535 (cit. on p. 140).

[256] Mohamed, S. A., Mahmoud, M. A., Mahdi, M. N., & Mostafa, S. A. (2022). Improving efficiency and effectiveness of robotic process automation in human resource management [Publisher: MDPI]. *Sustainability*, *14*(7), 3920. https://www.mdpi.com/2071-1050/14/7/3920 (cit. on p. 27).

[257] Mohammed, A. H., Abdulateef, A. A., & Abdulateef, I. A. (2021). Hyperledger, Ethereum and blockchain technology: A short overview. *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 1–6. https://doi.org/:10.1109/HORA52670.2021.9461294 (cit. on p. 107).

[258] Mohanty, D. (2018). Basic Solidity Programming, 55–103. https://doi.org/10.1007/978-1-4842-4075-5_3 (cit. on p. 107).

[259] Mohd Kamir, Y., & Md Yazid, S. (2016). The adoption and implementation of RFID : A literature survey. *Library and Information Science Research E-Journal*, *26*(1). https://doi.org/10.32655/LIBRES.2016.1.3 (cit. on p. 18).

[260] Moniz, H. (2020, May). The Istanbul BFT Consensus Algorithm. https://doi.org/10.48550/arXiv.2002.03613 (cit. on p. 114).

[261] Morales, D., Agudo, I., & Lopez, J. (2023). Integration of MPC into Besu through an extended private transaction model. *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, 266–273. https://doi.org/10.1109/MetaCom57706.2023.00056 (cit. on p. 110).

[262] Moreira, F. R., Da Silva Filho, D. A., Nze, G. D. A., de Sousa Júnior, R. T., & Nunes, R. R. (2021). Evaluating the performance of NIST's framework cybersecurity controls through a constructivist multicriteria methodology [Conference Name: IEEE Access]. *IEEE Access*, *9*, 129605–129618. https://doi.org/10.1109/ACCESS.2021.3113178 (cit. on p. 153).

[263] Morland, J. K. (1992). Review of a case for the case study [Publisher: Oxford University Press]. *Social Forces*, *71*(1), 240–242. https://doi.org/10.2307/2579984 (cit. on p. 149).

[264] Moshonas, S. (2018). *Power and policy-making in the DR Congo: The politics of human resource management and payroll reform* (tech. rep.). Universiteit Antwerpen, Institute of Development Policy (IOB). (Cit. on p. 23).

[265] Motshegwa, B., Mutonono, P., & Mikazhu, T. (2019). Embezzlement of the national petroleum fund in Botswana. http://ulspace.ul.ac.za/bitstream/handle/10386/2724/motshengwa_embezzlement_2019.pdf?sequence=1 (cit. on p. 19).

[266] Mouno, S. I., Rahman, T., Raatul, A. M., & afees Mansoor, N. (2024). Blockchain-enhanced academic certificate verification: A decentralized and trustworthy framework. *2024 International Conference on Advances in Computing, Communication, Electrical, and Smart Systems (iCACCESS)*, 1–5. https://ieeexplore.ieee.org/abstract/document/10499524/ (cit. on p. 55).

[267] Mouno, S. I., Rahman, T., Raatul, A. M., & Mansoor, N. (2023). Certiblock: The exemplary utilization of blockchain for the rigorous validation of academic certificates. *2023 26th International Conference on Computer and Information Technology (ICCIT)*, 1–6. https://ieeexplore.ieee.org/abstract/document/10441100/ (cit. on p. 55).

[268] Murch, M. (2017, July). Answer to "What does the nBits value represent?". https://bitcoin.stackexchange.com/a/57186 (cit. on p. 36).

[269] Mutula, S. M. (2001). Financing public universities in eastern and southern Africa: Implications for information services [Publisher: MCB UP Ltd]. *The Bottom Line*, *14*(3), 116–132. https://doi.org/10.1108/08880450110398681 (cit. on p. 17).

[270] Mutungi, F., Baguma, R., Janowski, T., & University Krems, D., Austria. (2019). Towards digital anti-corruption typology for public service delivery. *Proceedings of the 20th Annual International Conference on Digital Government Research*, 484–494. https://doi.org/10.1145/3325112.3325266 (cit. on p. 5).

[271] Nafiu, A. T., Yalo, M. I., & Aduku, D. J. (2016). Assessment of the variations of ghost employee fraud in Nigeria. *Assessment*, *8*(24) (cit. on pp. 1, 3, 4, 19).

[272] Nagtode, P. (2024). Research paper on transformative innovations in identity verification and recognition. *International Journal of Scientific Research In Engineering And Management*, *08*(05), 1–5. https://doi.org/10.55041/IJSREM35159 (cit. on p. 125).

[273] Nakajima, M. (2017). Essential elements of payment systems, 14. https://www.academia.edu/33639169/Essential_Elements_of_Payment_Systems (cit. on p. 16).

[274] Nakamoto, S. (2008a). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260 (cit. on p. 114).

[275] Nakamoto, S. (2008b). Re: Bitcoin P2P e-cash paper [Publisher: Nakamoto Institute Austin, TX, USA]. *The Cryptography Mailing List* (cit. on p. 28).

[276] Nasir, L. (2024, June). Strike: Organized labour suspends nationwide industrial action [Section: Nigeria]. https://von.gov.ng/strike-organized-labour-suspends-nationwide-industrial-action/ (cit. on p. 58).

[277] Nassaji, H. (2015). Qualitative and descriptive research: Data type versus data analysis. *Language Teaching Research*, *19*(2), 129–132. https://doi.org/10.1177/1362168815572747 (cit. on p. 86).

[278] Naz, M., Al-zahrani, F. A., Khalid, R., Javaid, N., Qamar, A. M., Afzal, M. K., & Shafiq, M. (2019). A Secure data sharing platform using blockchain and interplanetary file system. *Sustainability*, *11*(24), 7054. https://doi.org/10.3390/su11247054 (cit. on pp. 137, 138).

[279] Neu, J., Tas, E. N., & Tse, D. (2023). Accountable safety implies finality. *IACR Cryptol. ePrint Arch.*, *2023*, 1301. https://iacr.steepath.eu/2023/1301-AccountableSafetyImpliesFinality.pdf (cit. on p. 116).

[280] Neumann, J., Hoeller, N., Reinke, C., & Linnemann, V. (2010). Redundancy infrastructure for service-oriented wireless sensor networks. *2010 Ninth IEEE International Symposium on Network Computing and Applications*, 269–274. https://doi.org/10.1109/NCA.2010.50 (cit. on p. 114).

[281] Nguyen, P. T., & Nguyen, L. T. M. (2022). Understanding platform market value through decentralization governance—An integrative model from signaling and mechanism design theory [Publisher: Elsevier]. *Technological Forecasting and Social Change*, *183*, 121913. https://www.sciencedirect.com/science/article/pii/S0040162522004358?casa_token=a0 (cit. on p. 106).

[282] Nicoletti, L., Margheri, A., Lombardi, F., Sassone, V., & Schiavo, F. P. (2018). Cross-cloud management of sensitive data via Blockchain: A payslip calculation use case [Publisher: CEUR-WS. org]. https://eprints.soton.ac.uk/415084/ (cit. on p. 40).

[283] Nnamani, A. (2024, Aug.). ICPC exposes 22,074 suspicious workers in MDAs. https://thesun.ng/icpc-exposes-22074-suspicious-workers-in-mdas/ (cit. on p. 163).

[284] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain [Publisher: Springer]. *Business & Information Systems Engineering*, *59*(3), 183–187 (cit. on pp. 28, 30, 36).

[285] Noor, K. B. M. (2008). Case study: A strategic research methodology. *American journal of applied sciences*, *5*(11), 1602–1604. https://d1wqtxts1xzle7.cloudfront.net/98524637/ajassp.2008.1602-libre.pdf (cit. on p. 149).

[286] Nordrum, A. (2017). Govern by blockchain dubai wants one platform to rule them all, while Illinois will try anything. *IEEE Spectrum*, *54*(10), 54–55. https://doi.org/10.1109/MSPEC.2017.8048841 (cit. on p. 54).

[287] Nyaledzigbor, G. (2015). *Payroll fraud: Effects of ghost names on the government wage bill in Ghana* [PhD Thesis]. Walden University. (Cit. on pp. 57–59).

[288] Nyame, G., Qin, Z., Obour Agyekum, K. O.-B., & Sifah, E. B. (2020). An ECDSA approach to access control in knowledge management systems using blockchain [Publisher: MDPI]. *Information*, *11*(2), 111. https://www.mdpi.com/2078-2489/11/2/111 (cit. on p. 126).

[289] Obara, L. C., Nangih, E., & Agba, J. N. (2017). Accounting systems and payroll fraud in the public sector: A survey of selected ministries and parastatals in Rivers State, Nigeria. *Journal of Accounting and financial management*, *3*(2), 10–24. https://www.iiardjournals.org/get/JAFM/VOL.%203%20NO.%202%202017/ACCOUNTING%20SYSTEMS.pdf (cit. on p. 5).

[290] Obuah, E. (2010). Combating corruption in a "failed" state: The Nigerian Economic and Financial Crimes Commission (EFCC) [Publisher: Citeseer]. *Journal of Sustainable Development in Africa*, *12*(1), 27–53. https://d1wqtxts1xzle7.cloudfront.net/80764859/Combating_20Corruption_20in_20a_20Failed_20State-libre.pdf (cit. on p. 19).

[291] Ocampo, L. A., & Clark, E. E. (2014). Developing a framework for sustainable manufacturing strategies selection. *DLSU Business & Economics Review*, *23*(2), 115–131. https://d1wqtxts1xzle7.cloudfront.net/81344472/6clark-012014-libre.pdf (cit. on p. 153).

[292] Oguzierem, A., & Joab-Peterside, S. (2017). Ghost workers and related payroll fraud: The Impact of unauthorized employment on Local Government Areas (LGAS) & Rural Development Areas (RDAS) in Bayelsa state. *IIARD International Journal of Economics and Business Management*, *3*(8), 2489–0065 (cit. on pp. 75, 216).

[293] Olu-Adeyemi, O. (2018). 'E dibo, Ke Se Obe': 'Vote for cash' as an emergent paradigm of electoral corruption in Nigeria [Number: 2]. *African Research Review*, *12*(2), 13–22. https://doi.org/10.4314/afrrev.v12i2.2 (cit. on p. 22).

[294] Onukelobi, P. C., P., O., & V.C, P. (2019). Effects of financial management reforms on financial corruption in Nigeria public sector. *International Journal of Trend in Scientific Research and Development*, *3*(6), 839–852 (cit. on p. 2).

[295] Onyema, C. (2023). Extent of ICT usage and the effect on employee performance in Nigerian civil service. *Journal of Research in Humanities and Social Science*. https://www.questjournals.org/jrhss/papers/vol11-issue1/1101499504.pdf (cit. on p. 213).

[296] Or, C., & Chapman, E. (2021). An extended unified theory of acceptance and use of technology model for education contexts. *Journal of Applied Learning and Teaching*, *4*(2), 98–109. https://doi.org/doi.org/10.37074/jalt.2021.4.2.7 (cit. on p. 72).

[297] Otusajo, O., Aminu, I. Y., & Lateef, S. A. (2024). Role of treasury single account in the optimization of public sector funds in Nigeria. *FUDMA Journal of Accounting and Finance Research [FUJAFR]*, *2*(4), 60–73. https://www.fujafr.fudutsinma.edu.ng/index.php/fujafr/article/view/141 (cit. on p. 120).

[298] Oyelana, O., Kamanzi, J., & Richter, S. (2021). A critical look at exclusive breastfeeding in Africa: Through the lens of diffusion of innovation theory [Publisher: Elsevier]. *International Journal of Africa Nursing Sciences*, *14*, 100267. https://www.sciencedirect.com/science/article/pii/S221413912030144X (cit. on p. 69).

[299] Oyenuga Michael Oyedele, Ruth Angbazo Andah, & Nduji Romanus. (2023). Employee participation and organizational performance in an emerging econ-

omy. *Konfrontasi: Jurnal Kultural, Ekonomi dan Perubahan Sosial*, *10*(3), 135–149. https://doi.org/10.33258/konfrontasi2.v10i3.281 (cit. on p. 119).

[300] Pahlajani, S., Kshirsagar, A., & Pachghare, V. (2019). Survey on private blockchain consensus algorithms. *2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT)*, 1–6. https://doi.org/10.1109/ICIICT1.2019.8741353 (cit. on p. 34).

[301] Paik, H.-Y., Xu, X., Bandara, H. M. N. D., Lee, S. U., & Lo, S. K. (2019). Analysis of data management in blockchain-based systems: From architecture to governance [Conference Name: IEEE Access]. *IEEE Access*, *7*, 186091–186107. https://doi.org/10.1109/ACCESS.2019.2961404 (cit. on p. 36).

[302] Pal, A., Tiwari, C. K., & Behl, A. (2021). Blockchain technology in financial services: A comprehensive review of the literature [Publisher: Emerald Publishing Limited]. *Journal of Global Operations and Strategic Sourcing*, *14*(1), 61–80. https://doi.org/10.1108/JGOSS-07-2020-0039 (cit. on p. 29).

[303] Paliwal, M., & Saraswat, P. (2021). An overview on blockchain. *International Journal of Innovative Research in Computer Science & Technology*, *9*(6), 127–130. https://acspublisher.com/journals/index.php/ijircst/article/view/10946 (cit. on p. 126).

[304] Pan, R., Hu, Y., Liu, C., Li, K., & Li, K. (2023). Auction-based storage resource allocation for blockchain. *IEEE Internet of Things Journal*, *10*(24), 21607–21614. https://doi.org/10.1109/JIOT.2023.3304810 (cit. on p. 140).

[305] Pandey, P. (2018). Can blockchain spark off the reincarnation of India's living dead? *2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 1–8. https://ieeexplore.ieee.org/abstract/document/8855731/ (cit. on p. 54).

[306] Papernot, N., McDaniel, P., & Walls, R. J. (2015). Enforcing agile access control policies in relational databases using views. *MILCOM 2015-2015 IEEE Military Communications Conference*, 7–12. https://ieeexplore.ieee.org/abstract/document/7357410/ (cit. on p. 27).

[307] Patel, O. (2019). Building data replication system replication system IPFS nodes cluster. *International Journal of Science and Research (IJSR)*, *8*, 2057–2069. https://doi.org/10.21275/SR24708023552 (cit. on p. 140).

[308] Patton, E., & Appelbaum, S. H. (2003). The case for case studies in management research [Publisher: MCB UP Ltd]. *Management research news*, *26*(5), 60–71. https://www.emerald.com/insight/content/doi/10.1108/01409170310783484/full/html (cit. on p. 149).

[309] Paul, C., & Grace, F. O. (2020). Electronic governance and corruption in Nigeria: Combing insights from Integrated Payroll and Personnel Information System (IPPIS) implementation. https://ijidjournal.org/index.php/ijid/article/view/783 (cit. on p. 23).

[310] Peffers, K., Tuunanen, T., & Niehaves, B. (2018). Design science research genres: Introduction to the special issue on exemplars and criteria for applicable design science research. *European Journal of Information Systems*, *27*(2), 129–139. https://doi.org/10.1080/0960085X.2018.1458066 (cit. on p. 132).

[311] Petrossian, G. A., & Pezzella, F. S. (2018). IUU fishing and seafood fraud: Using crime script analysis to inform intervention. *The ANNALS of the American Academy of Political and Social Science*, *679*(1), 121–139. https://doi.org/10.1177/0002716218784533 (cit. on p. 159).

[312] Petter, S., DeLone, W., & McLean, E. R. (2013). Information systems success: The quest for the independent variables. *Journal of Management Information Systems*, *29*(4), 7–62. https://doi.org/10.2753/MIS0742-1222290401 (cit. on pp. 76, 77).

[313] Pothuri, V. V. (2024). Scalable and robust fraud detection in distributed systems. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, 103–107. https://www.ijarsct.co.in/Paper19519.pdf (cit. on p. 216).

[314] Prabhakar, S., Pankanti, S., & Jain, A. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, *1*(2), 33–42. https://doi.org/10.1109/MSECP.2003.1193209 (cit. on p. 27).

[315] Praitheeshan, P., Pan, L., & Doss, R. (2021). Private and trustworthy distributed lending model using Hyperledger Besu. *SN Computer Science*, *2*(2), 115. https://doi.org/10.1007/s42979-021-00500-3 (cit. on p. 110).

[316] Prusty, N. (2018). *Blockchain for Enterprise: Build scalable blockchain applications with privacy, interoperability, and permissioned features*. Packt Publishing Ltd. (Cit. on p. 111).

[317] Pupolizio, I. (2022). From Libra to Diem. The pursuit of a global private currency. *Global Jurist*, *22*(2), 281–306. https://doi.org/10.1515/gj-2021-0055 (cit. on p. 116).

[318] Puspitha, M. Y., & Yasa, G. W. (2018). Fraud pentagon analysis in detecting fraudulent financial reporting (study on Indonesian capital market). *International Journal of Sciences: Basic and Applied Research*, *42*(5), 93–109. https://core.ac.uk/download/pdf/249336574.pdf (cit. on p. 62).

[319] Quarm, R. S., & Rosemond, Q. (2020). Exorcising the'Ghosts' from the government payroll in developing countries in the wake of the COVID-19 pandemic: Ghana's empirical example. *Journal of Economics and Business*, *3*(4) (cit. on pp. 23, 214).

[320] Rabi'u, A., Mansor, N., & Muhammad, S. N. (2015). Fraud Triangle Theory and Fraud Diamond Theory. Understanding the Convergent and Divergent For Future Research. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, *5*. https://doi.org/10.6007/IJARAFMS/v5-i4/1823 (cit. on pp. 1, 58).

[321] Rafique, H., Almagrabi, A. O., Shamim, A., Anwar, F., & Bashir, A. K. (2020). Investigating the acceptance of mobile library applications with an extended technology acceptance model (TAM) [Publisher: Elsevier]. *Computers & Education*, *145*, 103732. https://www.sciencedirect.com/science/article/pii/S0360131519302854 (cit. on p. 72).

[322] Rahman, M. S., Khalil, I., Bouras, A., & Atiquzzaman, M. (2020). Design principles for migrating from traditional systems to blockchain systems. https://

blockchain.ieee.org/images/files/pdf/design-principles-for-migrating-from-traditional-systems-to-blockchain-systems_202001.pdf (cit. on p. 114).

[323] Rahman, M. U., Guidi, B., Baiardi, F., & Ricci, L. (2020). Context-aware and dynamic role-based access control using blockchain [Series Title: Advances in Intelligent Systems and Computing]. In L. Barolli, F. Amato, F. Moscato, T. Enokido, & M. Takizawa (Eds.), *Advanced Information Networking and Applications* (pp. 1449–1460, Vol. 1151). Springer International Publishing. https://doi.org/10.1007/978-3-030-44041-1_122 (cit. on p. 126).

[324] Ramesh, V. K. C. (2019). *Storing iot data securely in a private ethereum blockchain* [PhD Thesis]. University of Nevada, Las Vegas. https://search.proquest.com/openview/fba1ab0e990c6defa07ed4ab2b136cce/1?pq-origsite=gscholar&cbl=51922&diss=y (cit. on p. 114).

[325] Ramya, N., Kowsalya, A., & Dharanipriya, K. (2019). Service quality and its dimensions. *EPRA International Journal of Research & Development*, *4*(2), 38–41. https://eprajournals.com/IJSR/article/1196/abstract (cit. on p. 76).

[326] Rashid, M. A., Al-Mamun, A., Roudaki, H., & Yasser, Q. R. (2022). An overview of corporate fraud and its prevention approach. *Australasian Accounting, Business and Finance Journal*, *16*(1), 101–118. https://ro.uow.edu.au/aabfj/vol16/iss1/6/ (cit. on p. 157).

[327] Ratnasari, A., & Sudradjat, I. (2023). Case study approach in post-occupancy evaluation research. *ARTEKS: Jurnal Teknik Arsitektur*, *8*(3), 427–434. https://www.journal.unwira.ac.id/index.php/ARTEKS/article/view/2584 (cit. on pp. 148, 149).

[328] Reddy, R. G., Pateja, P. S., Patel, A., Palaniappan, G., & Rajendran, B. (2024). Identifying sybil attacks in blockchain networks through behavioral analysis and zero knowledge proof implementations. *2024 First International Conference on Data, Computation and Communication (ICDCC)*, 652–658. https://ieeexplore.ieee.org/abstract/document/10961103/ (cit. on p. 47).

[329] Reed, H., & Dailey, N. (2023). Decentralized approaches disrupt multi-stakeholder activities. *Disruptive Technologies in Information Sciences VII*, *12542*, 35–43. https://doi.org/10.1117/12.2665997 (cit. on p. 123).

[330] Regueiro, C., Seco, I., Gutiérrez-Agüero, I., Urquizu, B., & Mansell, J. (2021). A blockchain-based audit trail mechanism: Design and implementation [Publisher: MDPI]. *Algorithms*, *14*(12), 341. https://www.mdpi.com/1999-4893/14/12/341 (cit. on p. 125).

[331] Report, A. (2016). Annual Report. https://www.bpsr.gov.ng/en/resources/bpsr-resources/reports/annual-report/category/43-2016-annual-report (cit. on p. 5).

[332] Reynald, D. M. (2010). Guardians on guardianship: Factors affecting the willingness to supervise, the ability to detect potential offenders, and the willingness to intervene. *Journal of Research in Crime and Delinquency*, *47*(3), 358–390. https://doi.org/10.1177/0022427810365904 (cit. on pp. 63, 64).

[333] Reyns, B. W. (2017). Routine activity theory and cybercrime: A theoretical appraisal and literature review [Publisher: Routledge]. *Technocrime and criminological theory*, 35–54. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315117249-3/routine-activity-theory-cybercrime-bradford-reyns (cit. on p. 63).

[334] Riahi, K., Abouaissa, A., & Idoumghar, L. (2022). FPBFT: A fast PBFT protocol for private blockchains. *2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 1–8. https://ieeexplore.ieee.org/abstract/document/10062170/ (cit. on p. 35).

[335] Riney, F. A. (2018). Two-step fraud defense system: Prevention and detection [_eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/jcaf.22336]. *Journal of Corporate Accounting & Finance*, *29*(2), 74–86. https://doi.org/10.1002/jcaf.22336 (cit. on p. 57).

[336] Robson, C. (2002). *Real world research: A resource for social scientists and practitioner-researchers*. Wiley-Blackwell. (Cit. on p. 84).

[337] Ronald, M., Bradley, A., & Donna, W. (1997). Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. https://journals.aom.org/doi/abs/10.5465/amr.1997.9711022105 (cit. on p. 119).

[338] Rosenthal, A., & Sciore, E. (2000). View security as the basis for data warehouse security. *DMDW*, 8. http://www.tarrani.net/linda/ViewsAsBasis4DWSecurity.pdf (cit. on p. 27).

[339] Rosenthal, F. (1958). The Muqaddimah. *Jurnal Ushuluddin: An introduction to history*, *3*. https://www.academia.edu/41453145/THE_MUQADDIMAH#loswp-work-container (cit. on p. 1).

[340] Rot, A., & Blaicke, B. (2019). Blockchain's future role in cybersecurity. analysis of defensive and offensive potential leveraging blockchain-based platforms. *2019 9th International Conference on Advanced Computer Information Technologies (ACIT)*, 447–451 (cit. on pp. 42, 54).

[341] Rouse, E. D., & Harrison, S. H. (2015). Triangulate and expand: Using multiple sources of data for convergence and expansion to enrich inductive theorizing [Num Pages: 12]. In *Handbook of Qualitative Organizational Research*. Routledge. (Cit. on p. 154).

[342] Roworth-Stokes, S. (2011). The design research society and emerging themes in design research. *Journal of Product Innovation Management*, *28*(3), 419–424. https://doi.org/10.1111/j.1540-5885.2011.00815.x (cit. on pp. 128, 129).

[343] Rozario, A. M., & Vasarhelyi, M. A. (2018). Auditing with smart contracts. *The International Journal of Digital Accounting Research*, 1–27. https://doi.org/10.4192/1577-8517-v18_1 (cit. on p. 52).

[344] Rubino, F., Agostino, D., & Spallazzo, D. (2025). Strategizing blockchain adoption in public cultural services: A comprehensive scoping review [Publisher: Emerald Publishing Limited]. *International Journal of Public Sector Management*, *38*(1), 77–97. https://www.emerald.com/insight/content/doi/10.1108/ijpsm-12-2023-0383/full/html (cit. on p. 228).

[345] Ryan, B., & Gross, N. (1943). The diffusion of hybrid seed corn in two Iowa communities. *Rural Sociology*. https://www.proquest.com/openview/7de2b2276a089fe888071663de1
1?pq-origsite=gscholar&cbl=1817355 (cit. on p. 66).

[346] Sai, K., & Tipper, D. (2019). Disincentivizing double spend attacks across interoperable blockchains. *2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 36–45. https://doi.org/10.1109/TPS-ISA48467.2019.00014 (cit. on p. 120).

[347] Salihu, H. A., & Gholami, H. (2018). Corruption in the Nigeria judicial system: An overview [Publisher: Emerald Publishing Limited]. *Journal of Financial Crime*, *25*(3), 669–680. https://doi.org/10.1108/JFC-01-2017-0005 (cit. on p. 20).

[348] Salimitari, M., & Chatterjee, M. (2018). An overview of blockchain and consensus protocols for IoT networks. *arXiv preprint arXiv:1809.05613*, 1–12 (cit. on pp. 38, 39).

[349] Saltini, R., & Hyland-Wood, D. (2019, Sept.). IBFT 2.0: A safe and live variation of the IBFT blockchain consensus protocol for eventually synchronous networks. https://doi.org/10.48550/arXiv.1909.10194 (cit. on pp. 112, 114).

[350] Samuel, C. N., Glock, S., Verdier, F., & Guitton-Ouhamou, P. (2021). Choice of ethereum clients for private blockchain: Assessment from proof of authority perspective. *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 1–5. https://doi.org/10.1109/ICBC51069.2021.9461085 (cit. on p. 107).

[351] Samuel, O., & Augustine, A. (2022). Internal audit efficiency and fraud prevention: Empirical study of listed manufacturing companies in Nigeria. *08*(09). https://doi.org/10.47191/ijmei/v8i9.04 (cit. on pp. 1, 59, 89, 183, 218).

[352] Sanka, A. I., & Cheung, R. C. (2019). Blockchain: Panacea for corrupt practices in developing countries. *2019 2nd International Conference of the IEEE Nigeria Computer Chapter (NigeriaComputConf)*, 1–7. https://doi.org/10.1109/NigeriaComputConf45974.2019.8949626 (cit. on pp. 19, 39, 55).

[353] Sanka, A. I., Irfan, M., Huang, I., & Cheung, R. C. C. (2021). A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Computer Communications*, *169*, 179–201. https://doi.org/10.1016/j.comcom.2020.12.028 (cit. on pp. 32, 53).

[354] Santanu, K., Sen, Dey, S., & Saha, I. (2014). An innovative approach to devise security matrix to measure impact of attack vectors in cloud networks. *International Journal of Advance Research in Computer Science and Management Studies*. https://d1wqtxts1xzle7.cloudfront.net/67741051/IJARCSMS_All_Rights_Reserved_An_Innovati20210625 (cit. on p. 44).

[355] Saunders, M., Lewis, P., & Thornhill, A. (2007). Research methods. *Business Students 4th edition Pearson Education Limited, England* (cit. on pp. 84, 87, 90).

[356] Savovska, K. S., Vatyan, A., Danescu, D., & Crnkovic, L. (2018). Public sector internal audit : Focus on fraud. https://www.semanticscholar.org/paper/Public-Sector-Internal-Audit-%3A-Focus-on-Fraud-Savovska-Vatyan/154ee1df9f352174ec7772e7df672 (cit. on p. 121).

[357] Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack [Publisher: mdpi]. *Applied sciences*, *9*(9), 1788. https://www.mdpi.com/2076-3417/9/9/1788 (cit. on p. 42).

[358] Schuchter, A., & Levi, M. (2016). The Fraud Triangle revisited. *Security Journal*, *29*(2), 107–121. https://doi.org/10.1057/sj.2013.1 (cit. on pp. 1, 4, 6, 57).

[359] Schulte, P. (2018, Jan.). Chapter 13 - Mobile Technology: The new banking model connecting lending to the social network. In D. Lee Kuo Chuen & R. Deng (Eds.), *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2* (pp. 331–359). Academic Press. https://doi.org/10.1016/B978-0-12-812282-2.00013-9 (cit. on p. 17).

[360] Semenova, V. (2020). Technology adoption theories in examining the uptake of blockchain technology in the framework of functionalist and interpretive paradigms. *Vezetéstudomány/Budapest Management Review*, *51*(11), 26–38. https://doi.org/10.14267/VEZTUD.2020.11.03 (cit. on p. 69).

[361] Serena, L., Ferretti, S., & D'Angelo, G. (2021). Cryptocurrencies activity as a complex network: Analysis of transactions graphs. *Peer-to-Peer Networking and Applications*. https://doi.org/10.1007/s12083-021-01220-4 (cit. on p. 36).

[362] Shadnam, M., & Lawrence, T. B. (2011). Understanding widespread misconduct in organizations: An institutional theory of moral collapse [Publisher: Cambridge University Press]. *Business Ethics Quarterly*, *21*(3), 379–407. https://doi.org/10.5840/beq201121324 (cit. on p. 66).

[363] Shanks, G. (2002). Guidelines for conducting positivist case study research in information systems [Publisher: Australian Computer Society]. *Australasian Journal of Information Systems*, *10*(1). https://doi.org/10.3127/ajis.v10i1.448 (cit. on p. 149).

[364] Shevchenko, E., & Lunsford, R. (2023). Blockchain disruption in finance: JPMorgan Chase's success story and the transfer of Quorum to ConsenSys. *32* (cit. on p. 111).

[365] Shin, L. (2017). The first government to secure land titles on the bitcoin blockchain expands project. https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/ (cit. on pp. 5, 6, 53).

[366] Sicilia, M.-A., Garrido, P., Sánchez-Alonso, S., Mora-Cantallops, M., García-Barriocanal, E., Casquero, S., González, L., & Ballesteros, A. (2020). Qualified targeting through data aggregators in permissioned blockchain settings: A model for auditable transactions. In J. Prieto, A. Pinto, A. K. Das, & S. Ferretti (Eds.), *Blockchain and Applications* (pp. 111–120). Springer International Publishing. https://doi.org/10.1007/978-3-030-52535-4_12 (cit. on p. 111).

[367] Siddiq, F. R., & Sutopo, B. (2024). The Fraud Hexagon as an analytical framework for predicting financial statement fraud: A systematic literature review. *3*(2) (cit. on pp. 61–63).

[368] Sijan, P., & Sirish, P. (2018). Blockchain technology: A solution to plight of Nepalese migrant workers in foreign employment. https://ultraphysicalsciences.

org / paper / 1504 / blockchain - technology - a - solution - to - plight - of - nepalese - migrant-workers-in-foreign-employment (cit. on p. 118).

[369] Sikorski, J. J., Haughton, J., & Kraft, M. (2017). Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy*, *195*, 234–246. https://doi.org/10.1016/j.apenergy.2017.03.039 (cit. on p. 28).

[370] Simons, H. (2014). Case study research: In-depth understanding in context. *The Oxford handbook of qualitative research*, 455–470. https://books.google.com/books?hl=en&lr=&id=AzmTAwAAQBAJ&oi=fnd&pg=PA455&dq=Case+Study+Research:+In-Depth+Understanding+in+Context&ots=oR2r6FVjgE&sig=zXk_VtMQHg6upfnjkMWrxwrTgJ4 (cit. on p. 148).

[371] Singh, A., Parizi, R. M., Zhang, Q., Choo, K.-K. R., & Dehghantanha, A. (2020). Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. *Computers & Security*, *88*, 101654. https://doi.org/10.1016/j.cose.2019.101654 (cit. on pp. 71, 72).

[372] Singh, A., Chauhan, S. P. S., & Goel, A. K. (2023). Blockchain based verification of educational and professional certificates. *2023 2nd International Conference on Computational Systems and Communication (ICCSC)*, 1–7. https://ieeexplore.ieee.org/abstract/document/10143008/ (cit. on p. 54).

[373] Smith, K., & Dhillon, G. (2019). Improving the cybersecurity of financial transactions: Assessing blockchain potential. https://aisel.aisnet.org/amcis2019/treo/treos/1/ (cit. on p. 229).

[374] Soegoto, Y. (2019). Designing payroll information system: Case study on CV bandung ID card [Publisher: IOP Publishing]. *IOP Conference Series: Materials Science and Engineering*, *662*(2), 022125. https://doi.org/10.1088/1757-899X/662/2/022125 (cit. on p. 62).

[375] Son, D. H., Quynh, T. T. T., Khoa, T. V., Hoang, D. T., Trung, N. L., Ha, N. V., Niyato, D., Diep, N. N., & Dutkiewicz, E. (2021). An effective framework of private ethereum blockchain networks for smart grid. *2021 International Conference on Advanced Technologies for Communications (ATC)*, 312–317. https://doi.org/10.1109/ATC52653.2021.9598199 (cit. on p. 128).

[376] Stewart, A. (2019). Poster: GRANDPA Finality Gadget. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2649–2651. https://doi.org/10.1145/3319535.3363278 (cit. on p. 115).

[377] Stewart, P. (2014). Afghan police payroll under scrutiny from U.S. watchdog. *Reuters*. https://www.reuters.com/article/usa-afghanistan-police (cit. on pp. 5, 216).

[378] Strathcyber. (2024). StrathCyber — University of Strathclyde. https://www.strath.ac.uk/science/computerinformationsciences/strathcyber/ (cit. on p. 134).

[379] Sukendro, S., Habibi, A., Khaeruddin, K., Indrayana, B., Syahruddin, S., Makadada, F. A., & Hakim, H. (2020). Using an extended Technology Acceptance Model to understand students' use of e-learning during Covid-19: Indonesian sport science education context [Publisher: Elsevier]. *Heliyon*, *6*(11). https://www.cell.com/heliyon/pdf/S2405-8440(20)32253-2.pdf (cit. on p. 71).

[380] Sultana, S. A., Rupa, C., Malleswari, R. P., & Gadekallu, T. R. (2023). Ipfs-blockchain smart contracts based conceptual framework to reduce certificate frauds in the academic field [Publisher: MDPI]. *Information*, *14*(8), 446. https://www.mdpi.com/2078-2489/14/8/446 (cit. on p. 55).

[381] Sunny, J., Undralla, N., & Pillai, V. M. (2020). Supply chain transparency through blockchain-based traceability: An overview with demonstration [Publisher: Elsevier]. *Computers & Industrial Engineering*, *150*, 106895. https://doi.org/https://doi.org/10.1016/j.cie.2020.106895 (cit. on p. 229).

[382] Surendran, P. (2012). Technology Acceptance Model: A survey of literature [Number: 4]. *International Journal of Business and Social Research*, *2*(4), 175–178. https://doi.org/10.18533/ijbsr.v2i4.161 (cit. on pp. 70, 71).

[383] Sürücü, L., & Maslakçı, A. (2020). Validity and reliability in quantitative research. (Cit. on p. 90).

[384] Suryanto, S. (2011). Design and Analysis: Payroll of Accounting Information System. *CommIT (Communication and Information Technology) Journal*, *5*(1), 24–26. https://journal.binus.ac.id/index.php/commit/article/view/555 (cit. on p. 123).

[385] Swatzell, K., & Jennings, P. (2007). Descriptive research: The nuts and bolts [Publisher: LWW]. *JAAPA*, *20*(7). https://journals.lww.com/jaapa/fulltext/2007/07000/Descriptive_research__The_nuts_and_bolts.98.aspx (cit. on pp. 85, 86).

[386] Tagade, K. (2021, June). What is blockchain security? - Ultimate guide [Section: Knowledge Base]. https://www.getastra.com/blog/knowledge-base/blockchain-security/ (cit. on p. 42).

[387] Taherdoost, H. (2021). Data collection methods and tools for research; A step-by-step guide to choose data collection technique for academic and business research projects [Publisher: Helvetic Editions]. *International Journal of Academic Research in Management (IJARM)*, *10*(1), 10–38. https://hal.archives-ouvertes.fr/hal-03741847 (cit. on p. 86).

[388] Taiwo, A. A., & Downe, A. G. (2013). The theory of user acceptance and use of technology (UTAUT): A meta-analytic review of empirical findings. *Journal of Theoretical & Applied Information Technology*, *49*(1) (cit. on p. 72).

[389] Tan, D. (2017, Jan.). The Evolution of Payroll. https://www.affinityteam.com.au/the-evolution-of-payroll-full/ (cit. on p. 18).

[390] Tayal, A., Solanki, A., Kondal, R., Nayyar, A., Tanwar, S., & Kumar, N. (2021). Blockchain-based efficient communication for food supply chain industry: Transparency and traceability analysis for sustainable business. *International Journal of Communication Systems*, *34*(4), e4696. https://doi.org/10.1002/dac.4696 (cit. on p. 30).

[391] Thames, I. (2018). IPPIS Standard Operation Procedure. (Cit. on p. 24).

[392] Thomas, M., & Pierson, J. (2010). *Dictionary of social work: The definitive a to z of social work and social care*. McGraw-Hill Education (UK). (Cit. on p. 86).

[393] Tian, Y., Yang, C., Yang, J., & Nie, X. (2022). Efficient mobile vehicle data sharing scheme based on consortium blockchain [Number: 12 Publisher: Multidisciplinary Digital Publishing Institute]. *Applied Sciences*, *12*(12), 6152. https://doi.org/10.3390/app12126152 (cit. on p. 38).

[394] Toews, D. (2003). The New Tarde: Sociology after the end of the social theory culture and society. *Theory, Culture & Society*. https://doi.org/10.1177/02632764030205004 (cit. on p. 66).

[395] TransparencIT. (2017). TransparencIT - Corruption cases database in Nigeria. https://transparencit.com (cit. on p. 163).

[396] TransparencIT, A. (2020). TransparencIT - Corruption cases database in Nigeria. https://transparencit.com (cit. on pp. 6, 163).

[397] Trojanowski, M., & Kułak, J. (2019). A literature review of the classic and extended Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) model [Publisher: Polskie Wydawnictwo Ekonomiczne]. *Marketing i Rynek*, (7), 3–18. https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ojs-doi-10_33226_1231-7853_2019_7_1 (cit. on p. 73).

[398] Tsiaras, K. (2023). Study and resource analysis of ethereum execution client bootstrapping. https://dspace.lib.ntua.gr/xmlui/bitstream/handle/123456789/57592/Tsiaras_thesis.pdf?sequence=1 (cit. on p. 107).

[399] Uddin, M., Salah, K., Jayaraman, R., Pesic, S., & Ellahham, S. (2021). Blockchain for drug traceability: Architectures and open challenges. *Health Informatics Journal*, *27*(2), 14604582211011228. https://doi.org/10.1177/14604582211011228 (cit. on p. 128).

[400] Uesugi, T., Shijo, Y., & Murata, M. (2021). Design and Evaluation of a Privacy-preserving Supply Chain System Based on Public Permissionless Blockchain. *2021 International Symposium on Electrical, Electronics and Information Engineering*, 312–321. https://doi.org/10.1145/3459104.3459155 (cit. on p. 30).

[401] Ullah, N., Mugahed Al-Rahmi, W., Alzahrani, A. I., Alfarraj, O., & Alblehai, F. M. (2021). Blockchain technology adoption in smart learning environments [Publisher: MDPI]. *Sustainability*, *13*(4), 1801. https://doi.org/10.3390/su13041801 (cit. on p. 69).

[402] Unacedemy. (2022). Applied vs Fundamental Research. https://unacademy.com/content/upsc/study-material/psychology/applied-vs-fundamental-research/ (cit. on p. 83).

[403] Urien, P., Dandjinou, M., & Agbezoutsi, K. E. (2018). BTOOLS: Trusted transaction generation for bitcoin and ethereum blockchain based on crypto currency smartCard (cit. on p. 114).

[404] Uroos, A., Shabbir, M. S., Zahid, M. U., Yahya, G., & Abbasi, B. A. (2022). Economic analysis of corruption: Evidence from Pakistan. *Transnational Corporations Review*, *14*(1), 46–61. https://doi.org/10.1080/19186444.2021.1917331 (cit. on p. 19).

[405] Us, D. o. J. (2023, Oct.). Former nursing home worker charged with wire fraud in "ghost" employee fraud scheme. https://www.justice.gov/opa/pr/former-nursing-home-worker-charged-wire-fraud-ghost-employee-fraud-scheme (cit. on p. 171).

[406] Uzoh, B. C. (2020). Academic Staff Union of Universities (ASUU) And The Politics of Integrated Payroll and Personnel Information System (IPPIS) In Nigerian Federal Universities. *Economics and Social Sciences Academic Journal*, *2* (cit. on pp. 5, 22–24).

[407] Vaishnavi, V. K. (2007). *Design science research methods and patterns: Innovating information and communication technology*. Auerbach Publications. https://www.taylorfrancis.com/books/mono/10.1201/9781420059335/design-science-research-methods-patterns-vijay-vaishnavi (cit. on p. 129).

[408] Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences*, *15*(3), 398–405. https://doi.org/10.1111/nhs.12048 (cit. on p. 154).

[409] Van Teijlingen, E., & Hundley, V. (2001). The importance of pilot studies. *Social research update*, (35), 1–4. http://eprints.bournemouth.ac.uk/10149/ (cit. on p. 89).

[410] Varela, M., Lopes, P., & Rodrigues, R. (2021). Rigour in the management case study method: A study on master's dissertations. *Electronic Journal of Business Research Methods*, *19*(1), pp1–13. https://academic-publishing.org/index.php/ejbrm/article/view/2072 (cit. on p. 149).

[411] Vaus, D. D. (2013, Dec.). *Surveys in social research* (6th ed.). Routledge. https://doi.org/10.4324/9780203519196 (cit. on p. 87).

[412] Venkatesh, V., Thong, J. Y., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the association for Information Systems*, *17*(5), 328–376. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2800121 (cit. on pp. 72, 73).

[413] Verma, S., & Sheel, A. (2022). Blockchain for government organizations: Past, present and future. *Journal of Global Operations and Strategic Sourcing*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/JGOSS-08-2021-0063 (cit. on p. 29).

[414] Vona, L. W. (2012). *Fraud risk assessment: Building a fraud audit program*. John Wiley & Sons. (Cit. on p. 57).

[415] Vousinas, G. L. (2019). Advancing theory of fraud: The S.C.O.R.E. model. *Journal of Financial Crime*, *26*(1), 372–381. https://doi.org/10.1108/JFC-12-2017-0128 (cit. on p. 62).

[416] Wallis, K., Schillinger, F., Reich, C., & Schindelhauer, C. (2019). Safeguarding data integrity by cluster-based data validation network. *2019 Third World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4)*, 78–86. https://doi.org/10.1109/WorldS4.2019.8904039 (cit. on p. 123).

[417] Wang, X. (2024). Blockchain security and applications: A comprehensive analysis from hash functions to consensus algorithms. *Theoretical and Natural Science*, *31*(1), 292–298. https://doi.org/10.54254/2753-8818/31/20240862 (cit. on p. 126).

[418] Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management*, *52*, 102090. https://doi.org/10.1016/j.ijinfomgt.2020.102090 (cit. on p. 29).

[419] Wegrzyn, K., & Wang, E. (2021). Types of blockchain: Public, private, or something in between — Foley & Lardner LLP. https://www.foley.com/en/insights/

publications / 2021 / 08 / types - of - blockchain - public - private - between (cit. on p. 40).

[420] Wells, J. T. (2017). *Corporate fraud handbook: Prevention and detection*. John Wiley & Sons. (Cit. on pp. 1, 4).

[421] Wikimedia. (2017). Replay attack on hash. https://commons.wikimedia.org/wiki/File:Replay_attack_on_hash.svg (cit. on p. 46).

[422] Wikipedia. (2022, May). Walter Onnoghen [Page Version ID: 1088235529]. https://en.wikipedia.org/w/index.php?title=Walter_Onnoghen&oldid=1088235529 (cit. on p. 22).

[423] Wilcox, P., & Cullen, F. T. (2018). Situational opportunity theories of crime. *Annual Review of Criminology*, *1*(1), 123–148. https://doi.org/10.1146/annurev-criminol-032317-092421 (cit. on p. 63).

[424] Wilcox, P., Land, K., & Hunt, S. A. (2018). *Criminal circumstance: A dynamic multi-contextual criminal opportunity theory*. Routledge. https://www.taylorfrancis.com/books/mono/10.4324/9780203794364/criminal-circumstance-kenneth-land-pamela-wilcox-scott-hunt (cit. on p. 63).

[425] Wilhelm, W. K. (2004). The fraud management lifecycle theory. *Journal of economic crime management*, *2*(2), 1–38 (cit. on pp. 74, 75).

[426] William, D., & Ephraim, M. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. *Journal of Management Information Systems*, *19*(4), 9–30. https://doi.org/10.1080/07421222.2003.11045748 (cit. on pp. 76, 77).

[427] Witman, P. (2007). Banking regulatory response - The case of strong authentication. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1986&context=amcis2007 (cit. on p. 149).

[428] Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *Kennesaw State University*. https://digitalcommons.kennesaw.edu/facpubs/1537/ (cit. on pp. 60, 61).

[429] Wood, G., & Steiner, J. (2016). Trustless computing—The what not the how [Series Title: New Economic Windows]. In P. Tasca, T. Aste, L. Pelizzon, &

N. Perony (Eds.), *Banking Beyond Banks and Money* (pp. 133–144). Springer International Publishing. https://doi.org/10.1007/978-3-319-42448-4_8 (cit. on p. 32).

[430] Wust, K., & A, G. (2018). Do you need a blockchain? *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 45–54. https://doi.org/10.1109/CVCBT.2018.00011 (cit. on p. 37).

[431] Xiaojie, Z. (2017). The faculty salary system of the medieval university. *Chinese Studies in History*, *50*(1), 14–23. https://doi.org/10.1080/00094633.2016.1227540 (cit. on p. 17).

[432] Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A survey of blockchain technology applied to smart cities: Research issues and challenges [Conference Name: IEEE Communications Surveys & Tutorials]. *IEEE Communications Surveys & Tutorials*, *21*(3), 2794–2830. https://doi.org/10.1109/COMST.2019.2899617 (cit. on pp. 33–35).

[433] Xiong, H., Chen, M., Wu, C., Zhao, Y., & Yi, W. (2022). Research on progress of blockchain consensus algorithm: A review on recent progress of blockchain consensus algorithms [Number: 2 Publisher: Multidisciplinary Digital Publishing Institute]. *Future Internet*, *14*(2), 47. https://doi.org/10.3390/fi14020047 (cit. on pp. 32, 35, 109).

[434] Xu, X., Weber, I., & Staples, M. (2019). *Architecture for blockchain applications*. Springer International Publishing. https://doi.org/10.1007/978-3-030-03035-3 (cit. on p. 29).

[435] Yang, Y., Lin, T., Liu, P., Zeng, P., & Xiao, S. (2022). UCBIS: An improved consortium blockchain information system based on UBCCSP. *Blockchain: Research and Applications*, *3*(2), 100064. https://doi.org/10.1016/j.bcra.2022.100064 (cit. on p. 39).

[436] Yemi, E. (2022). FG detects 1,500 fake workers in civil service. https://www.thisdaylive.com/index.php/2022/04/06/fg-detects-1500-fake-workers (cit. on p. 2).

[437] Yeoh, P. (2017). Regulatory issues in blockchain technology [Publisher: Emerald Publishing Limited]. *Journal of Financial Regulation and Compliance*, *25*(2), 196–208. https://doi.org/10.1108/JFRC-08-2016-0068 (cit. on p. 29).

[438] Yin, M., Malkhi, D., Reiter, M. K., Gueta, G. G., & Abraham, I. (2019). HotStuff: BFT consensus with linearity and responsiveness. *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing*, 347–356. https://doi.org/10.1145/3293611.3331591 (cit. on p. 116).

[439] Yu, J., Zhang, X., Wang, J., Zhang, Y., Shi, Y., Su, L., & Zeng, L. (2024). Robust and trustworthy data sharing framework leveraging on-chain and off-chain collaboration. *Computers, Materials & Continua*, *78*(2). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=15462218&AN=175815010&h=lYW5t3dPQ19ns (cit. on p. 140).

[440] Yusuf, Z., Nawawi, A., & Salin, A. S. A. P. (2020). The effectiveness of payroll system in the public sector to prevent fraud. *Journal of Financial Crime*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/JFC-08-2017-0075 (cit. on pp. 89, 183).

[441] Zalukhu, A. A. J., & Reskino, R. (2024). Analysis of Fraud Hexagon Theory on fraudulent financial reporting based on the role of intellectual capital as a mediator that is influenced by earnings management practices. *Co-Value Jurnal Ekonomi Koperasi dan kewirausahaan*, *15*(1). http://journal.ikopin.ac.id/index.php/covalue/article/view/4444 (cit. on p. 62).

[442] Zhao, G., Liu, S., Lopez, C., Lu, H., Elgueta, S., Chen, H., & Boshkoska, B. M. (2019). Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions. *Computers in Industry*, *109*, 83–99. https://doi.org/10.1016/j.compind.2019.04.002 (cit. on pp. 28, 41).

[443] Zhao, W., Yang, S., & Luo, X. (2019). On Consensus in Public Blockchains. *Proceedings of the 2019 International Conference on Blockchain Technology*, 1–5. https://doi.org/10.1145/3320154.3320162 (cit. on p. 34).

[444] Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey [Publisher: Inderscience Publishers (IEL)].

*International Journal of Web and Grid Services*, *14*(4), 352–375 (cit. on pp. 31, 52, 139, 216).

[445] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *2017 IEEE international congress on big data (BigData congress)*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85 (cit. on pp. 36, 108).

[446] Zohal, H. (2014). Political corruption, public procurement, and budget composition: Theory and evidence from OECD countries [Publisher: Elsevier]. *European Journal of political economy*, *34*, 372–389. https://www.sciencedirect.com/science/article/pii/S017626801400024X?casa_token=vkFXtOoUdqgAAAAA (cit. on p. 59).

[447] Zucker, L. G. (1987). Institutional theories of organization [Publisher: JSTOR]. *Annual review of sociology*, *13*, 443–464. https://www.jstor.org/stable/2083256 (cit. on p. 66).

[448] Zulfan, Z. (2018). An information system success model for cloud computing in information technology project [Number: 1]. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *2*(1), 18–36. https://doi.org/10.22373/cs.v2i1.2661 (cit. on p. 77).

[449] Zwitter, A., & Hazenberg, J. (2020). Decentralized network governance: Blockchain technology and the future of regulation [Publisher: Frontiers]. *Frontiers in Blockchain*, *3*. https://doi.org/10.3389/fbloc.2020.00012 (cit. on p. 106).

# Appendix A

# 2021 Ethics Application

# CIS Ethics Approval System

*You are Musa Bello (Research Student - 202077359)*

Return to Main

Application ID: 1527

Title of research:
Improving Payroll Systems In Developing Countries Using Blockchain Technologies

Summary of research (short overview of the background and aims of this study):
Payroll management is an essential process for every organization with staff, as payment of staff should be accurate and timely (Singh et al., 2017). However, the payment platforms in the developing countries are filled with grave defects such as accepting of ghost workers (fake employees), conflicting of salaries (where Mr. A receives the salary of Mr. B) and centralization. In Nigeria, the Federal Government is currently using the defective (Aluko, 2020) Integrated Payroll and Personnel Information System (IPPIS) as a payroll platform to pay its employees (Uzoh, 2020). This system violates university autonomy by removing the power to recruit competent, local and foreign scholars as it is with global practice (Aluko, 2020).
Employments are completely shifted to the Office of the Accountant General of the Federation (AGF) which gives rise to Ghost Workers and lots of abnormalities (Uzoh, 2020). This leads to serious negative impacts on government parastatals, educational institutions, economic and social growth (Bamigboye et al., 2016). The aim of this study is to use blockchain capabilities to improve payroll system in developing countries. Analysis of existing literature will be presented. Case study research methodology will be used for the investigation. Data will be collected from secondary and primary sources. Secondary data on the payroll system development will be collected from the office of the Accountant General of the Federation in Nigeria. Primary data will be collected by conducting in depth interviews with IPPIS personnel. Questionnaires will be administered to staff under IPPIS platform to capture their views on IPPIS. The research at the end will bridge a gap and improve our understanding of blockchain, payroll, cyber security, and economic growth.

How will participants be recruited?
Participants comprise of academic and non-academic staff of Federal universities whose salaries are being paid through the Integrated Personnel and Payroll Information System (IPPIS) platform. The questionnaires shall be administered through Qualtrics Survey engine.
The participants for the interview are only the IPPIS staff. They shall be contacted at the Office of the Accountant General of the Federation-Nigeria. They are responsible for the smooth running and operation of the IPPIS application. It will be a face to face session where the researcher ask and then transcribe the response.

If you are using IPPIS personnel for interviews and questionnaires then you need to complete this whole form.

What will the participants be told about the proposed research study? Either upload or include a copy of the briefing notes issued to participants. In particular this should include details of yourself, the context of the study and an overview of the data that you plan to collect, your supervisor, and contact details for the Departmental Ethics Committee.
PDF File: View document
Please find attached document
You need to create a Participant Information Sheet that clearly outlines the study, expectations of participants, data management, contact details etc - please see the ethics pages for templates to use to construct this appropriately following the standard question and answer format.

This Participant Information Sheet is more along the lines of what is required but is still not quite there yet - please follow the traditional Question and Answer format for this document. You will find examples of these via the CIS ethics page and University ethics page. Please also ensure your Supervisor has had a chance to review and approve documentation prior to re-submission.

How will consent be demonstrated? Either upload or include here a copy of the consent form/instructions issued to participants. It is particularly important that you make the rights of the participants to freely withdraw from the study at any point (if they begin to feel stressed for example), nor feel under any pressure or obligation to complete the study, answer any particular question, or undertake any particular task. Their rights regarding associated data collected should also be made explicit.
PDF File: View document
Please find attached document
These statements need to be revised into appropriate consent statements - it may be easier to create this as a standalone consent form document that you can then include on the opening page to your survey. Again, please review the ethics pages carefully for templates and advice on creating appropriate consent forms.

What will participants be expected to do? Either upload or include a copy of the instructions issued to participants along with a copy of or link to the survey, interview script or task description you intend to carry out.

PDF File: None.
PDF File: None.
This is the copy of the link of the proposed survey https://strath.eu.qualtrics.com/jfe/form/SV_6KmSpZjx12OSMyG
The questions for the interview which is specifically targeted at the IPPIS staff

Open Ended Interview Questions Intended For IPPIS Personnel
1. How many people involved in the Payroll Process?
2. How many users operating the IPPIS application?
3. Who are the people approving the online transaction payment?
4. How is the transaction approved?
5. What are the roles of the top management when considering approvals?
6. Who is/are responsible for creating User Profile?
7. Who is/are responsible for effecting corrections?
8. Can you tell me the beginning of the payroll process?
9. Where and how do you start entering/modifying data in the application?
10. What are the reports/outputs generated from the system?
11. What are the problems do you usually encounter during operations?
12. How do you normally fix these errors?

You may wish to add not applicable as an option to your survey responses.
Your cover page for the survey will need to be updated when you provide a corrected and revised consent form and information sheet.

What data will be collected and how will it be captured and stored? In particular indicate how adherence to the Data Protection Act and the General Data Protection Regulation (GDPR) will be guaranteed and how participant confidentiality will be handled.
Qualitative and Quantitative data will be collected through conducting interviews and administering questionnaires. The raw data data obtained shall be stored in Microsoft Excel format and shall be analysed through Statistical Package for Social Sciences (SPSS). All research data will be stored on central university-approved storages (OneDrive).
There are two aspects of data collection. One of them requires participants to fill questionnaires. There are twenty one questions in the questionnaire. Each question is followed by five options which participants are to choose one. Here is the link https://strath.eu.qualtrics.com/jfe/form/SV_6KmSpZjx12OSMyG

The second part is the interview which will be directed only to staff of IPPIS. There are twelve open-ended questions. It will be a face to face session where the researcher ask and then transcribe the response. I will personally do the interviewing and do the transcribing. The recording shall be on saved at that moment on my computer system, properly encrypted. Later after analysis it shall be transferred unto the central university-approved storages (OneDrive) where it will remain up to ten years.
It is not clear how you are conducting, recording, transcribing and storing interview data - please revise

Still more transparency and clarity required please on storage of recording and transcriptions. Also, who is doing the transcriptions - please specify this given potential issues around data access.

How will the data be processed? (e.g. analysed, reported, visualised, integrated with other data, etc.) Please pay particular attention to descibing how personal or sensitive data will be handled and how GDPR regulations will be met.
The raw data obtained through questionnaires shall be analysed through Statistical Package for Social Sciences (SPSS). Reports from the SPSS application shall be interpreted and analysed graphically while some on tables.

The questions for the interview are mainly qualitative in nature, clear and open-ended. The idea is to have a background on the functionalities and process of IPPIS. This will enable me to have a guide on how flowchart will be formulated and presented. So there is no formal processing of interview questions, only pictorial representation of how the system works would be developed.

As above - some more clarity and transparency about data analysis for the qualitative data particularly is needed - how will you analyse this data, where will it be stored, who will have access to it etc?

How and when will data be disposed of? Either upload a copy of your data management plan or describe how data will be disposed.
PDF File: None.
Data will be archived in line with the University of Strathclyde's Research Data Management Policy. Data for this particular research will be retained up to ten years on the central university-approved storages (OneDrive). External users will be bound by data sharing agreement of the university and a consent form will be signed in that regard.

What is the funders policy? What does this mean for how your data will be stored, accessed, shared etc? Is this any different to the University policy and if so, how will this be managed?

What is the rationale for storing data indefinitely? How does this concur with guidelines and why is it different for this project?
Please seek support from your supervisor prior to resubmission.

Supervisor's name (students should complete this question).

☐ I confirm that my supervisor has seen and approved both my planned study and this associated ethics application.

# Appendix B

# 2021 Ethics Approval Email

Outlook

## Ethics application has been approved

**From** www-data@cis.strath.ac.uk <www-data@cis.strath.ac.uk>
**Date** Mon 06/09/2021 17:31
**To** Musa Bello <musa.bello@strath.ac.uk>

Hello,

Your ethics application "Improving Payroll Systems In Developing Countries Using Blockchain Technologies" (ID: 1527) has been approved.

URL: https://local.cis.strath.ac.uk/wp/extras/ethics/index.php?view=1527

CIS Ethics Approval System.

# Appendix C

# 2021 Participant Information Sheet

# Participant Information Sheet for Musa Ibrahim Bello

**Name of department: Computer and Information Sciences**
**Title of the study: Improving Payroll Systems In Developing Countries Using Blockchain Technologies**

**Introduction**

Musa Ibrahim Bello, a first-year research student from the department of Computer and Information Science, University of Strathclyde, United Kingdom, is carrying out a PhD research on the need for improving payroll systems in developing countries using blockchain technology.

**What is the purpose of this research?**

The aim of the study is to use blockchain capabilities to design a framework that will improve the Payroll systems in developing countries, particularly the Nigerian payroll platform - Integrated Payroll and Personnel Information System (IPPIS). The Federal Government of Nigeria is currently using the platform to pay its employees

**Do you have to take part?**

The involvement of any participant in this research is solely voluntary. Participants have absolute right to withdraw at any stage of the research. Participants as well can skip any question he/she is not comfortable with and that will not affect the participant in any way.

**What will you do in the project?**

There are two aspects of data collection. One of them requires participants to fill questionnaires. There are twenty one questions in the questionnaire. Each question is followed by five options which participants are to choose one. The second part is the interview which will be directed only to staff of IPPIS. There are twelve open-ended questions. It will be a face to face session where the researcher ask and then transcribe the response.

**Why have you been invited to take part?**

Participants comprise of academic and non-academic staff of Federal universities whose salaries are being paid through the Integrated Personnel and Payroll Information System (IPPIS) platform.

**What information is being collected in the project?**
The information collected will inform the researcher the present situation of IPPIS and how is actually being perceived by enrolees. This may include its effectiveness, strength, or weakness. Personal or identifiable data will not in any way be captured as the exercise will remain anonymous. Both the interview and online survey will not ask any of the participants' personal details.

**Where will the information be stored and how long will it be kept for?**
Data will be archived in line with the University of Strathclyde's Research Data Management Policy. Data for this particular research will be retained up to ten years on the central university-approved storages (OneDrive) as it is an anonymous research data.

**What happens next?**

Any participant who is interested in the findings of this research after it is completed or published should not hesitate to contact Musa Ibrahim Bello on mobile phone +2348033556111 or by email: musa.bello@strath.ac.uk and a consent form will be signed in that regard. I appreciate your consent to contribute to this important research. I also thank those who could not get involved in this research for their intention and encouragements.

Yours sincerely,

Musa Ibrahim Bello
Department of Computer and Information Science
University of Strathclyde,
Glasgow.
United Kingdom
+447425175062
Email: musa.bello@strath.ac.uk

Project Supervisor
Dr. Daniel Thomas
Department of Computer and Information Science
University of Strathclyde,
Glasgow.
United Kingdom
Email: d.thomas@strath.ac.uk

Secretary to the Departmental Ethics Committee
Department of Computer and Information Sciences,
University of Strathclyde,
Livingstone Tower
Richmond Street
Glasgow
G1 1XH
Email:ethics@cis.strath.ac.uk

# Appendix D

# 2021 Consent Form

# Consent Form for Academic and Non-Academic Staff of Federal Universities, Nigeria.

**Name of Department**: Computer and Information Sciences

**Title of Study**: Improving Payroll Systems in Developing Countries Using Blockchain Technologies

- I confirm that I have read and understood the Participant Information Sheet for the above project and the researcher has answered any queries to my satisfaction.
- I confirm that I have read and understood the Privacy Notice for Participants in Research Projects and understand that my personal information will not be involved in any way
- I understand that my participation is voluntary and that I am free to withdraw from the project at any time, up to the point of completion, without having to give a reason and without any consequences.
- I understand that anonymised data (i.e. data that do not identify me personally) cannot be withdrawn once they have been included in the study.
- I understand that any information recorded in the research will remain confidential and no information that identifies me will be made publicly available.
- I consent to being a participant in the project.

| | |
|---|---|
| Signature of Participant: | Date: |

# Appendix E

# 2024 Ethics Application

# CIS Ethics Approval System

*You are Musa Bello (Research Student - 202077359)*

Return to Main

Application ID: 2764

Title of research:
Enhancing Employment Integrity Process to Curb Ghost Worker Fraud Using Blockchain Technology

Summary of research (short overview of the background and aims of this study):
The primary concern of this study is the widespread problem of ghost workers in Nigeria's public sector and the urgent necessity to tackle this type of fraudulent activity. This study is motivated by the substantial financial losses and inefficiencies resulting from ghost worker fraud in the employment process. This fraudulent activity undermines public trust and depletes resources that are intended for legitimate employees and other public projects. The Nigerian government implemented the Integrated Personnel and Payroll Information System (IPPIS) as a way to improve the payroll management and employment process of the federal civil service by increasing transparency, accountability, and efficiency. Despite the implementation, the ghost worker issue has not been totally resolved. The system is still being exploited by fraudsters, who fabricate bogus employee records and steal public funds covertly.
Despite the implementation of the IPPIS, fraud involving the employment process which leads to ghost worker fraud remains a serious obstacle for Nigeria's public sector. False employee records are created by dishonest individuals who take advantage of IPPIS vulnerabilities, which causes both financial loss and a decline in public confidence. In order to improve transparency, accountability, and security inside the public employment process that will reduce ghost worker fraud, it is urgently necessary to investigate novel solutions. Therefore, the aim of this research is to design a framework that could improve transparency within the employment process and curb ghost worker fraud in Nigeria by integrating blockchain technology and external organizations with the existing IPPIS.

How will participants be recruited?
Participants comprise of the employees of the Federal Government of Nigeria, Government Employee, blockchain expert or private sector employee. The questionnaires shall be administered through Qualtrics Survey engine. Equally, participants will be contacted via various WhatsApp groups, facilitating easier recruitment and outreach to a large number of potential respondents.

What will the participants be told about the proposed research study? Either upload or include a copy of the briefing notes issued to participants. In particular this should include details of yourself, the context of the study and an overview of the data that you plan to collect, your supervisor, and contact details for the Departmental Ethics Committee.
PDF File: View document

1. Please include the section: "Who will have access to the information?" in the Participant Information Sheet.
For example, if personal information will be shared with any individuals or organizations outside the University, details of the external recipients should be provided. This includes any external transcription services or open access to data.
2. Please include the section: " Why have you been invited to take part?" in the Participant Information Sheet.

How will consent be demonstrated? Either upload or include here a copy of the consent form/instructions issued to participants. It is particularly important that you make the rights of the participants to freely withdraw from the study at any point (if they begin to feel stressed for example), nor feel under any pressure or obligation to complete the study, answer any particular question, or undertake any particular task. Their rights regarding associated data collected should also be made explicit.
PDF File: None.
Here is the link of the proposed survey: https://strath.eu.qualtrics.com/jfe/form/SV_9Y3qFHLAmxrPdZ4
Please add the sections regarding participant's printed name, signature, and date to the consent form.

What will participants be expected to do? Either upload or include a copy of the instructions issued to participants along with a copy of or link to the survey, interview script or task description you intend to carry out.
PDF File: None.
PDF File: None.
Here is the link of the proposed survey: https://strath.eu.qualtrics.com/jfe/form/SV_9Y3qFHLAmxrPdZ4
The link provided here shows the Participant Information Sheet, not the survey. Please double-check.

What data will be collected and how will it be captured and stored? In particular indicate how adherence to the Data Protection Act and the General Data Protection Regulation (GDPR) will be guaranteed and how participant confidentiality will be handled.
Quantitative data will be collected through administering questionnaires on Qualtrics. The raw data data obtained shall be stored in .scv format and shall be analysed through Statistical Package for Social Sciences (SPSS). All research data will be stored on central university-approved storages (OneDrive).
There is one aspect of data collection in which participants are required to fill out questionnaires. There are twenty-five questions in the questionnaire. Each question is followed by options which participants are to choose one. Here is the link: https://strath.eu.qualtrics.com/jfe/form/SV_9Y3qFHLAmxrPdZ4

The link provided here shows the Participant Information Sheet, not the questionnaire. Please double-check.

How will the data be processed? (e.g. analysed, reported, visualised, integrated with other data, etc.) Please pay particular attention to descibing how personal or sensitive data will be handled and how GDPR regulations will be met.
The raw data shall be analysed through Statistical Package for Social Sciences (SPSS). Reports from the SPSS application shall be interpreted and analyzed graphically, while some on tables.

How and when will data be disposed of? Either upload a copy of your data management plan or describe how data will be disposed.
PDF File:  None.
Data will be archived in line with the University of Strathclyde's Research Data Management Policy. Data for this particular research will be retained up to ten years on the central university-approved storages (OneDrive). External users will be bound by data sharing agreement of the university and a consent form will be signed in that regard.

Supervisor's name (students should complete this question).

☑ I confirm that my supervisor has seen and approved both my planned study and this associated ethics application.

# Appendix F

# 2024 Ethics Approval Email

Outlook

## Ethics application has been approved

**From** Ethics Approval System <do-not-reply@cis.strath.ac.uk>
**Date** Mon 09/12/2024 14:06
**To** Musa Bello <musa.bello@strath.ac.uk>

Hello,

Your ethics application "Enhancing Employment Integrity Process to Curb Ghost Worker Fraud Using Blockchain Technology" (ID: 2764) has been approved.

URL: https://local.cis.strath.ac.uk/wp/extras/ethics/index.php?view=2764

CIS Ethics Approval System.

# Appendix G

# 2024 Participant Information Sheet

# Participant Information Sheet for Musa Ibrahim Bello

**Name of department:** Computer and Information Sciences
**Title of the study:** Enhancing Employment Integrity Process to Curb Ghost Worker Fraud Using Blockchain Technology

**Introduction**

Musa Ibrahim Bello, a PhD student from the department of Computer and Information Science, University of Strathclyde, United Kingdom, is carrying out research on Enhancing Employment Integrity Process to Curb Ghost Worker Fraud Using Blockchain Technology

**What is the purpose of this research?**

This survey's main goal is to compile opinions and ideas on a proposed blockchain framework for assessment from government employees and professionals. Your opinion will help us better understand the feasibility, potential benefits, evaluation, and challenges of deploying this technology in the public sector.

The proposed decentralised validation framework seeks to improve the integrity and transparency of employment processes by allowing for the secure sharing of employee data among relevant government agencies, including the Central Bank of Nigeria (CBN), the Integrated Personnel and Payroll Information System (IPPIS), and various ministries. Implementing a networked system helps to greatly lower the possibility of ghost worker fraud by allowing real-time validation of employee identities and status. Ghost worker fraud involves creating fake personnel records to siphon salary income.

The framework's key components include stakeholder collaboration, decentralised data sharing, access control and security, and feedback mechanism, employees, and technology providers to combine and develop a transparent approach to data and employment validation.

This framework is aimed to bring increased transparency in the employment process, better detection and curbing of ghost worker fraud.

As an expert or government employee, your knowledge and views are vital to this study. Your answers will offer important details on how blockchain technology could be included into current employment procedures and how it could solve present issues with data security, transparency, and fraud prevention.

**Do you have to take part?**

The involvement of any participant in this research is solely voluntary. Participants have absolute right to withdraw at any stage of the research. Participants as well can skip any question they are not comfortable with and that will not affect the participant in any way.

**What will you do in the project?**

The questionnaire contains 22 questions and should take about 6 to 8 minutes to complete. Kindly respond to every question the best you could. We really value your insightful and honest answers.

**What information is being collected in the project?**

The information collected will serve as a pilot study which will assist and inform the researcher how clear, relevant and easy to understand the survey questions regarding how employees of the federal government of

Nigeria and experts' perception of IPPIS and its relation to ghost worker fraud and evaluate the proposed Blockchain Validation Framework. Personal or identifiable data will not in any way be captured as the exercise will remain anonymous.

**Where will the information be stored and how long will it be kept for?**

Data will be archived in line with the University of Strathclyde's Research Data Management Policy. Data for this particular research will be retained for up to ten years on the central university-approved storages (OneDrive) as it is an anonymous research data.

**What happens next?**

Any participant who is interested in the findings of this research after it is completed or published should not hesitate to contact Musa Ibrahim Bello, email: musa.bello@strath.ac.uk. I appreciate your consent to contribute to this important research. I also thank those who could not get involved in this research for their intention and encouragement.

**Researcher contact details:**
Musa Ibrahim Bello
Department of Computer and Information Sciences
University of Strathclyde, Glasgow.
United Kingdom
musa.bello@strath.ac.uk

Project Supervisor
Dr. Daniel Thomas
Department of Computer and Information Sciences
University of Strathclyde, Glasgow.
United Kingdom
d.thomas@strath.ac.uk

This research was granted ethical approval by the Computer & Information Sciences Ethics Committee.

If you have any questions/concerns, during or after the research, or wish to contact an independent person to whom any questions may be directed or further information may be sought from, please contact:

cis-ml-ethics-committee@ds.strath.ac.uk

# Appendix H

# 2024 Consent Form

**Employees of Federal Government of Nigeria and Experts in Blockchain**
**Name of Department:** Department of Computer and Information Sciences
**Title of the Study:** Enhancing Employment Integrity Process to Curb Ghost Worker Fraud Using Blockchain Technology

▪ I confirm that I have read and understood the Participant Information Sheet for the above project and the researcher has answered any queries to my satisfaction.
▪ I understand that my participation is voluntary and that I am free to withdraw from the project at any time, up to the point of completion, without having to give a reason and without any consequences.
▪ I understand that my responses are anonymous
▪ I understand that any information recorded in the research will remain confidential and no information that identifies me will be made publicly available.
▪ I understand that the Department of Computer and Information Sciences Ethics Committee, University of Strathclyde, United Kingdom (ethics@cis.strath.ac.uk) has approved this study

- o I consent to participate in the project

- o No, I DO NOT consent to participate in the project