



**APPLICATION OF BLOCKCHAIN TECHNOLOGY FOR DATA SECURITY: CASE
STUDY OF GLOBAL MISSION SERVICES' DIGITAL PLATFORM**

by

Yves Ndayisenga Bizumuremyi

Dissertation submitted in fulfilment of the degree

MASTER IN INFORMATION TECHNOLOGY

in the

Faculty of Engineering, Built Environment and Information Communication
Technology

Department of Information Technology

at the

Central University of Technology, Free State

Supervisor: Dr Ntima Mabanza

Co-supervisor: Prof. Masinde Muthoni

2024

Copyright Notice

This dissertation is to be used only for academic and non-commercial research purposes. The information contained in this dissertation is to be published with acknowledgement of the source. The rights of this dissertation are held by the author. This dissertation is published by the Central University of Technology, Free State, in terms of a non-exclusive license granted to CUT by the author.

Disclaimer

The presentation of this dissertation contains colour images meant to present results visually in a more understandable form. While printing or viewing this dissertation in grey scale (black and white) is possible, it is recommended that for clarity the dissertation is viewed (or printed) in full-colour format.

Declaration

I, **Yves Ndayisenga Bizumuremyi**, identity number ##### and student number #####, do hereby declare that this research project submitted to the Central University of Technology, Free State, for the qualification Master of Information Technology, is my own independent work; complies with the Code of Academic Integrity, as well as other relevant policies, procedures, rules and regulations of the Central University of Technology, Free State, and has not been submitted before to any institution by myself or any other person in fulfilment (or partial fulfilment) of the requirements for the attainment of any qualification.

Yves Ndayisenga Bizumuremyi

Signature: _____

Date: _____

In our capacity as supervisors of this dissertation, we certify that the above statements are true to the best of our knowledge.

Dr Ntima Mabanza

Signature: _____

Prof. Masinde Muthoni

Signature: _____

Dedication

This dissertation is dedicated to my late father, Zacharie Bizumuremyi, my mother, Busenene Leontine and my uncle and guardian, Canisius Bisangwa.

Acknowledgements

First and foremost, I would like to express my heartfelt gratitude for the divine guidance of Almighty God, who has illuminated my path throughout this journey. I am deeply grateful to my heavenly mother Mary for all her graces and intercessions. A profound and special thank you is extended to my cherished family. To my mother, Busenene Leontine, your continuous prayers have been my guiding light. To my late father, Zacharie Bizumuremyi, who inspired me to work hard and avoid all anti-values. To my uncle and guardian, Canisius Bisangwa, from whom I learnt to persevere and never give up. To my brothers and sisters, your constant support and encouragement encouraged me to strive for excellence.

I would also like to express my heartfelt gratitude to all the missionaries who participated in the study. A particular thanks to Paul Fotoh for his essential assistance in the early phases of my research. His wise advice on Global Mission Services helped shape my study. In addition, I would like to express sincere gratitude to the international student office, particularly Mrs CeeCee Sejake, for the continuous support she has graciously provided. To all those who contributed to completing this dissertation, my friends, data collectors, analysts, and proof-readers, your assistance has been significant, and I am profoundly grateful for your contributions.

Last but certainly not least, I sincerely thank my esteemed supervisors, Dr Ntima Mabanza and Prof. Muthoni Masinde. Your patience, understanding, and guidance have been instrumental in shaping this work. With humility, I acknowledge your invaluable contributions to my journey of growth and learning.

Abstract

In the contemporary digital era, the security of online data is a critical concern for organisations, institutions, and individuals. With the rapid proliferation of digital platforms, particularly in service-based sectors, safeguarding sensitive information has become paramount. This dissertation explores the application of blockchain technology for enhancing data security on a service-based digital platform, focusing specifically on the Global Mission Services (GMS) platform, which integrates accommodation and logistics services for missionaries in South Africa and Eswatini.

The motivation for this research stems from the challenges faced by missionaries in locating secure and affordable accommodation during their travels. These challenges are exacerbated by the lack of synergy among different missionary networks, which often operate independently and within their own congregations. Existing digital platforms like Airbnb and Booking.com are not tailored to the unique needs of missionaries and do not offer the required level of data security, particularly when sensitive information is stored in the cloud.

Blockchain technology, known for its decentralised, transparent, and tamper-resistant nature, offers a promising solution to these challenges. This research aims to develop and implement a blockchain-based framework to secure data on the GMS digital platform, thereby enhancing the platform's confidentiality, integrity, and availability (CIA). The research addresses the identified gaps in the existing literature, particularly the lack of practical applications of blockchain in securing data on service-based platforms.

The study adopts a mixed-methods approach through an explanatory sequential design. Quantitative data were first collected and analysed to identify the requirements and perceptions of the target users' missionaries regarding online data security. This was followed by qualitative analysis to gain deeper insights into the findings. The Design Science Research Methodology (DSRM) was employed to guide the development of the Blockchain framework, ensuring that it meets the specific needs of the GMS platform.

Key components of the research include a comprehensive literature review and bibliometric analysis of existing digital platforms and their business models, as well as an in-depth study of blockchain technology and its application in data security. The developed framework was tested on the GMS platform using Ethereum, a public blockchain that supports smart contracts and decentralised applications (DApps). System testing involved the use of various web resources including Interplanetary File System (IPFS), Hardhat, Polygon, Infura, and MetaMask to evaluate the platform's adherence to the CIA Triad.

The findings of this study demonstrate that blockchain technology can significantly enhance the security of service-based digital platforms. This was proven through the literature review and confirmed by the system testing. The GMS platform, when secured with Blockchain, showed improved data integrity, transparency, and decentralisation, which are critical for building trust among missionaries and facilitating the efficient use of accommodation resources. The research also highlights the potential of Blockchain to lower operational costs by streamlining the management of multiple systems under a single, secure digital platform.

This dissertation contributes to the growing body of knowledge on the use of blockchain technology for data security, particularly in the context of service-based platforms in developing countries. The practical framework developed in this study provides a robust solution that can be adapted to similar contexts, addressing the broader challenge of securing sensitive data in the digital age.

Publications resulting from research

- I. Bizumuremyi, Y., Mabanza, N. and Masinde, M. (2022), “Bibliometric Analysis of the Application of Blockchain Technology for Data Security: a Case Study of Global Mission Services’ Digital Platform”, 2022 IST-Africa Conference, IST-Africa 2022, Institute of Electrical and Electronics Engineers Inc., doi: 10.23919/IST-AFRICA56635.2022.9845628.

- II. Bizumuremyi, Y., Mabanza, N. and Masinde, M. (2024), “Adopting Blockchain for Enhancing Data Security and Privacy in Service-Based Digital Platforms: A Case Study of a Distributed Application (Dapp) Global Mission Services”. AFRICATEK 2023. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 520. Springer, Cham, pp. 57–70, doi: 10.1007/978-3-031-63999-9_4.

Table of Contents

Copyright Notice	i
Disclaimer	ii
Declaration.....	iii
Dedication.....	iv
Acknowledgements.....	v
Abstract.....	vi
Publications resulting from research	viii
List of Figures	xii
List of Tables	xiii
List of abbreviations and acronyms	xiv
1. CHAPTER 1: Introduction and Background Information	1
1.0. Introduction	1
1.1. Research Problem.....	3
1.2. Research Questions	4
1.3. Research Aims and Objectives.....	4
1.4. Research Methodology.....	5
1.5. Research Limitations.....	5
1.6. Research Contribution	6
1.7. Dissertation Structure	7
2. CHAPTER 2: Literature Review	8
2.0. Introduction	8
2.1. Missionaries	8
2.1.1. Missionaries' definition.....	8
2.1.2. Missionaries' activities.....	8
2.1.3. Current missionaries' travel logistics.....	9
2.2. Digital Platforms.....	10
2.2.1. Digital platforms definition	10
2.2.2. Service-based digital platforms	10
2.2.3. Existing travel-logistics digital platforms.....	11
2.2.4. Service-based digital platforms data security raised issues	13
2.3. Data Security Frameworks	15
2.3.1. Data security framework definition	15
2.3.2. Overview of various data security frameworks	15
2.4. Blockchain Technology	21

2.4.1.	Blockchain technology definition	21
2.4.2.	Blockchain classification	22
2.4.3.	Blockchain technology architecture	23
2.4.4.	Application of blockchain technology	23
2.4.5.	Existing blockchain frameworks	25
2.4.6.	Blockchain technology for data security for digital platforms	27
2.4.7.	Blockchain technology to guarantee data security	28
2.4.8.	Blockchain technology for developing secured digital platforms	30
2.5.	Related work	37
2.6.	Summary	42
3.	CHAPTER 3: Research Methodology	43
3.0.	Introduction	43
3.1.	Research Paradigm	43
3.2.	Research Methodology	44
3.2.1.	Mixed-methods design	44
3.2.2.	Design Science Research Methodology	45
3.3.	Case Study of Missionaries in Eswatini and South Africa	47
3.3.1.	Research setting	47
3.3.2.	Sampling techniques	47
3.3.3.	Participants	48
3.3.4.	Data collection techniques	49
3.3.5.	Validity and reliability	51
3.3.6.	Data analysis	52
3.4.	Summary	53
4.	CHAPTER 4: Framework Development Process	54
4.0.	Introduction	54
4.1.	The Framework's Rationale	54
4.2.	Blockchain Framework Building Process	55
4.2.1.	Phase 1: Identification of the problem	55
4.2.2.	Phase 2: Definition of objectives for a solution	55
4.2.3.	Phase 3: Design and development of the blockchain framework for data security	56
4.2.4.	Phase 4: Demonstration	61
4.2.5.	Phase 5: Evaluation	61
4.2.6.	Phase 6: Communication	61

4.3. Conclusion.....	62
5. CHAPTER 5: Framework Implementation.....	63
5.0. Introduction	63
5.1. Framework Demonstration.....	63
5.1.1. Specification requirements of the GMS.....	63
5.1.2. Blockchain technology implementation of CIA Triad	70
5.1.3. Architecture design	71
5.1.4. System design	72
5.1.5. Prototype implementation	77
5.2. Data Security Evaluation	80
5.2.1. Testing procedures	81
5.3. Summary.....	89
6. CHAPTER 6: Discussion, Conclusion, and Future Work	90
6.0. Introduction	90
6.1. Significant findings.....	90
6.1. Reflection.....	92
6.1.1. Scientific reflection	92
6.1.2. Substantive reflection	93
6.1.3. Methodological reflection	93
6.2. Lessons Learned.....	94
6.3. Future Considerations.....	95
6.4. Concluding Remarks	96
References.....	98
Appendices.....	113
Appendix 1: Selection Questionnaire	113
Appendix 2: Online Security and Website Usage Questionnaire	116
Appendix 3: Consent Form	119
Appendix 4: Ethical Clearance.....	120
Appendix 5: Graphs.....	121
Appendix 6: Confirmation of Proofreading.....	123
Appendix 7: Smart Contracts Source code	124

List of Figures

Figure 2.1. An overview of blockchain architecture (Casino et al., 2019).....	23
Figure 2.2 Bitcoin block construction using the Merkle Tree (Balaskas and Franqueira, 2018).....	26
Figure 2.3. Ethereum framework architecture	31
Figure 2.4. Building blocks of a blockchain	32
Figure 2.5. Blockchain example	33
Figure 2.6. IPFS Structure.....	36
Figure 4.1. The Design Science Research.....	55
Figure 4.2. Blockchain framework for data security in digital platform components ..	56
Figure 4.3. Framework architecture design	58
Figure 4.4. Blockchain technology framework using CIA Triad model architecture ..	60
Figure 5.1. GMS decentralised architecture	71
Figure 5.2. Authentication flowchart	72
Figure 5.3. Data integrity flowchart.....	73
Figure 5.4. Availability flowchart.....	74
Figure 5.5. GMS use case diagram.....	75
Figure 5.6. Sequence diagram of GMS digital platform.....	76
Figure 5.7. Class diagram	77
Figure 5.8. Hardhat local server accounts.....	78
Figure 5.9. MetaMask account	79
Figure 5.10. Deployed contract information.....	79
Figure 5.11. GMS home page, missions section.....	80
Figure 5.12. Private key generated by MetaMask	82
Figure 5.13. Mission Dashboard/Centre Profile.....	83
Figure 5.14. Booking page	83
Figure 5.15. Transaction details and activity log	84
Figure 5.16. Data validation testing results	85
Figure 5.17. Mission contract verification results.....	86
Figure 5.18. Accommodation contract verification results	86
Figure 5.19. Seamless Integration of Infura IPFS ensures secure and reliable data storage	87
Figure 5.20. The deployment and testing results	88
Figure 5.21. Fleek deployment summary	89
Figure 0.1. Centre's geographical location	121
Figure 0.2. Frequency of centres with a functional website and the number of years they have been operating.....	121
Figure 0.3. The number of centres and the generated monthly revenue.....	122
Figure 0.4. Website usage purpose	122

List of Tables

Table 4.1. Scholars utilising the CIA Triad in their work	17
Table 3.1. Design science process (Hevner & Park, 2004)	46
Table 5.1. Online security data.....	66
Table 6.1. Significant findings	91
Table 6.2. Research questions, answers, and evidence	97

List of abbreviations and acronyms

AAA	Authorisation, Authentication, and Accounting
ACM	Association for Computing Machinery
CIA	Confidentiality, Integrity, and Availability
CUT	Central University of Technology, Free State
DApp	Decentralised Application
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
DRS	Design Research Science
EVM	Ethereum Virtual Machine
FEBIT	Faculty of Engineering, Built Environment, and Information Technology
GDPR	General Data Protection Regulation
Geth	Go-Ethereum
GMS	Global Mission Services
HIPAA	Health Insurance Portability and Accountability Act
IEEE	Institute of Electrical and Electronics Engineers
IPFS	Interplanetary File System
ISO/IEC 27001	International Organisation for Standardisation/International Electrotechnical Commission 27001 (Information Security Management System)
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
PoW	Proof of Work

1. CHAPTER 1: Introduction and Background Information

1.0. Introduction

Online presence benefits organisations, institutions, and businesses by increasing visibility, improving operational efficiency, and contributing to overall growth (Cioppi, Curina, Forlani and Pencarelli, 2019). Nowadays, many organisations, institutions and businesses use websites and social media to promote their operations (Cioppi *et al.*, 2019; Dwivedi, Ismagilova, Rana and Raman, 2021). Others adopt shared economy platforms like Amazon, Alibaba, Airbnb, and Booking.com to expand their customer base and improve their operations. These platforms redefine how companies interact with stakeholders and do business by utilising available resources and skills to create value, which promotes economic interchange (Duan, 2023). In this digital age, it is vitally important for all kinds of businesses, no matter their size, to have an online presence. However, there are still businesses or organisations that are lagging or are reluctant in embracing the concept of an online presence. For example, missionaries in Eswatini and South Africa run missionary centres that provide essential services to the community. Accommodations such as retreat, and workshop centres are one example of those services. Consequently, there are still many people who are unaware of this service due to limited information availability. Different causes contribute to this. Currently, missionaries in South Africa and Eswatini only share services within their congregations. The results of the survey that was conducted in this research revealed that some of these missionary centres have websites that facilitate booking and advertising of their accommodation facilities, as well as other activities related to their mission, but the majority of people who are not part of their congregation are not aware of this information. Another possible cause is that missionaries use the Southern African Catholic Bishops' Conference directory (SACBC, 2024), which includes a list of some missionary centres as well as retreat and workshop facilities. However, the directory does not offer booking options or provide full details.

Taking into account the aforementioned, it becomes clear that there is a need for an integrated platform that brings together all these missionary centres and facilitates finding the different accommodations that they provide.

As mentioned earlier, there are numerous shared economy digital platforms available, such as Airbnb, Booking.com and many more. However, since missionaries operate as non-governmental organisations, they find it difficult to join these platforms. Furthermore, an integrated digital platform may increase access and utilisation of these resources, although storing data on the cloud raises concerns about privacy breaches (Ahmed et al., 2019).

These days, the security of information online has become a critical concern for individuals, organisations, and governments worldwide. Sensitive information is being shared and stored online as the use of digital devices, cloud computing, and the internet grows, making it vulnerable to cyber threats such as data breaches, hacking, and ransomware attacks. These threats cost billions of dollars to both small and large businesses and organisations each year (Oghene, 2023). This demonstrates how much the risk of a data breach is increasing, as is the risk of online data, which is a massive liability for organisations. Hence, it is vital to establish critical cyber security measures to protect sensitive data from cyber-attacks. To overcome this challenge in the case of missionaries in South Africa and Eswatini, a novel system that provides trust and data integrity for the service-based digital platform is required to allow a safe exchange of accommodation services among missionaries in Eswatini and South Africa.

Blockchain technology is one example of such promising novel cyber security measure solutions for protecting sensitive data from cyber-attacks. Blockchain is the most disruptive technological advancement from the fourth industrial revolution. Blockchain research is developing fast, and blockchain technology is anticipated to serve as the main engine for the upcoming generation of digital platforms (Mohammed *et al.*, 2021).

Taking the above into consideration, the current research explores the application of blockchain technology for data security, focusing on a case study of the Global Mission Services (GMS) digital platform. This platform development intends to integrate all missionary accommodation facilities, including retreat and workshop centres, as well as provide information on various missionary activities. The focal point of this research is to investigate blockchain technology's potential for data security within the GMS digital platform. The study explicitly assesses the efficacy of blockchain technology in

assuring data confidentiality, integrity, and availability in the context of the GMS digital platform.

1.1. Research Problem

It has been found that, when travelling, missionaries encounter many challenges in settling and adapting to new environments, including safety issues, accommodation, transportation, and others (Bučko, 2013). The result of an interview done by the researcher, with missionaries travelling to Eswatini and South Africa reveal that they have difficulty locating safe and reasonably priced accommodation. They frequently struggle to trust their surroundings because they are new to the area. This is a serious challenge for missionaries hoping to carry out their mission in the region.

On the other hand, and as mentioned earlier, many missionaries provide accommodation services such as retreat and workshop facilities, which may aid other missionaries and people in their network. However, those in need of these services are often unaware of these useful facilities. While some missionary centres have websites, they function independently and share services within the same congregations, making it difficult for visiting missionaries to locate these resources. This situation indicates a lack of synergy across various missionary networks. Furthermore, missionary organisations often operate under non-governmental organisation (NGO) structures, and this prevents them from joining profit-driven service-rendering digital platforms such as Booking.com and Airbnb due to the platforms' commercial orientation and registration requirements.

It is well known that service-based digital platforms face several cyber security treats. Möller (2020), Qammar, Karim, Ning and Ding (2023) also confirmed that most current service-based platforms face substantial data security concerns. Blockchain technology is one example of promising novel cyber security measure solutions for protecting sensitive data from cyber-attacks. Taylor, Dargahi, Dehghantanha, Parizi and Choo (2020), Qammar et al. (2023) and Moosavi and Taherdoost (2023) confirmed that there are very few systematic literature reviews on the application of blockchain in developing data security frameworks. Hence, the current research aims to fill this gap by exploring what needs to be improved more, especially in service-based platforms such as the GMS.

1.2. Research Questions

The following three research questions were formulated based on the problem statement:

- 1) What are the benefits of implementing a digital platform for Global Mission Services?
- 2) How has blockchain technology transformed the technology industry?
- 3) To what extent is blockchain technology effective for developing a data security framework?

1.3. Research Aims and Objectives

This research aimed to investigate the feasibility of using blockchain technology in developing a framework for securing data for service-based digital platforms. The success of this framework was then tested on a travel-logistics services digital platform for missionaries. This was achieved by pursuing the following research objectives:

1. To carry out a comprehensive literature review and bibliometric analysis of how the existing digital platforms transform business models and architectures to identify the most applicable one for a service-based digital platform for missionaries. To this end, the following aspects are covered:
 - a) Detailed study and analysis of missionary travels and operations.
 - b) Literature review and bibliometric analysis of the application of blockchain technology in developing a data security framework.
 - c) A review of existing security framework models.
2. Design a framework that uses blockchain to secure data for service-based digital platforms.
3. Develop a service-based digital platform prototype that meets requirements for activities for selected missionary institutions in South Africa and Eswatini. This includes the booking and advertisement of retreat centres and workshop centres offered by missionary centres.
4. To evaluate the effectiveness of the framework developed in sub-objective 2 on the GMS digital platform developed in sub-objective 3 to ensure that the information is secured. The findings of this study will be used to recommend a

method for incorporating the platform in a way that improves its security and effectiveness.

1.4. Research Methodology

This study adopted a mixed-method approach through an explanatory sequential design. Initially, quantitative data were collected and analysed, followed by the collection and analysis of qualitative data. The quantitative phase was utilised to select participants, while the qualitative phase delved deeper into exploring participants' perceptions regarding the security of their online data. By combining both qualitative and quantitative methodologies, a holistic understanding of participants' requirements was achieved. A range of data collection techniques, including surveys and system testing, was employed to ensure the precision of the data. Multiple data sources relevant to the research objectives were incorporated to enhance the validity and reliability of the findings. Additionally, the rationale behind the selection of the methodologies and protocols was clearly articulated to align with the study's aims and objectives. The qualitative and quantitative data was analysed using R Studio. Conclusions were drawn based on the results of comparative statistical test analyses conducted by the researcher.

1.5. Research Limitations

This research analyses the use of blockchain technology to reinforce data security in the context of service-based digital platforms. The study compares blockchain to traditional security techniques to evaluate the extent to which it can improve data security on the GMS digital platform. However, it is crucial to acknowledge that the study has the following limitations.

- First, because the framework developed in this study was applied to the GMS digital platform with just the features and functionalities required for the aim of this research, it may be harder to generalise the findings to other businesses or situations.
- Secondly, the participants were missionaries from Eswatini and South Africa. This focus may limit the findings' generalisability to other locations or groups.
- Lastly, the testing of the system prototype was carried out through the Ethereum online platform. The following web resources were involved: IPFS,

Hardhat, Polygon, Infura for Polygon, and MetaMask. Testing took place only within these tools and platforms; thus, it did not fully reflect the diversity of the potential environment in which the system could be deployed.

1.6. Research Contribution

This study covers three aspects (Confidentiality, Integrity and Availability) of data security in service-based digital platforms, notably the GMS digital platform. To this end, it contributes to the understanding of how blockchain technology can be utilised to improve data security, and trust among missionaries and facilitate access to accommodation services provided by missionary centres in Eswatini and South Africa. This was accomplished through:

- Firstly, by developing a blockchain framework for data security following the CIA Model for service-based digital platforms, specifically in the context of missionary accommodation services. The developed Blockchain framework aims to overcome the limitations of traditional data security methods; by improving security through decentralisation, immutability, consensus mechanisms, smart contracts, and transparency.
- Secondly, the developed Blockchain framework was tested and implemented on the GMS digital platform using Ethereum, a public blockchain that supports smart contracts and decentralised applications. System testing was carried out to assess the effectiveness of the developed blockchain framework in securing service-based digital platforms.

The findings of this study help improve the development, service delivery and security in similar setups, contributing to a larger improvement in digital platform efficacy in developing countries. To the best knowledge of the researcher, very little is known about studies that focus on the application of blockchain technology and developed data security frameworks in service-based digital platforms, especially in the context of missionaries in Eswatini and South Africa. Therefore, this study is the first to lay a foundation for the understanding of how to integrate blockchain technology to improve data security travel-logistic digital platforms and service delivery for missionaries in Eswatini and South Africa. This study makes a valuable positive contribution to the growing body of research on blockchain technology.

1.7. Dissertation Structure

The current dissertation consists of six chapters. Chapter 1 offers an introduction to the research study. The objective for the research is explained, along with the research problem and questions. The research design and method, limitations and, finally, the contribution and structure of the research study are briefly discussed. Chapter 2 draws upon a comprehensive literature review of missionaries in South Africa and Eswatini. The types of services they provide and the current state of how they exchange their services are explored. Additionally, the practical application of blockchain technologies to enhance data security in service-based digital platforms is discussed. In assessing the viability of blockchain technology towards ensuring data confidentiality, integrity and availability, this study investigates its potential advantages and challenges regarding securing data. Chapter 3 presents an in-depth assessment of the research methodology and justifies its use. The outline of this study's data collection, analysis and procedures are also presented. The proposed blockchain technology framework is presented in Chapter 4, and the prototype of the GMS digital platform development and evaluation is provided in Chapter 5. Chapter 6 concludes the research by summarising the study. This chapter considers the research's reflections, findings and makes recommendations for future research in the domain of blockchain technology for data security in a service-based digital platform.

2. CHAPTER 2: Literature Review

2.0. Introduction

This chapter examines how blockchain technology can be used to enhance data security on service-based digital platforms. The goal of this literature review is to identify current techniques and frameworks used in data security for service-based digital platforms. Additionally, it looks at how blockchain technology can be integrated with the already-existing service-based platforms. A comprehensive analysis of the role played by Catholic missionaries in society, their activities, and the potential of blockchain technology to secure data on digital platforms is also done. The review also covers current technical developments in this area and focuses on the initiatives taken by academics to overcome gaps in the literature.

2.1. Missionaries

2.1.1. Missionaries' definition

Caggiano (2022) defines a missionary as somebody who loves and follows Jesus wherever they are, while showing love to others in the way they live. Through their missionary activities, they contribute to serving and developing communities. Maxwell (2014) attests that missionary movements and actions have significantly impacted many people's lives worldwide and have largely shaped world history. Missionaries are found everywhere on the globe. However, this research study focuses on missionaries in South Africa and Eswatini.

2.1.2. Missionaries' activities

Missionaries in South Africa and Eswatini provide a range of services in various fields or industries, such as health care services, education, environment, accommodation and feeding of people experiencing homelessness, rehabilitation of people involved in substance abuse, refugee assistance, early child development programmes, running of orphanages, combating human trafficking, communication, as well as in community development projects through cooperatives and public benefit companies. Among the listed range of services provided, including accommodation, the travelling logistics facilities, specifically, will be the focus of this research study.

2.1.3. Current missionaries' travel logistics

All missionary centres in South Africa and Eswatini have accommodation facilities, conference centres and retreat places. People from other congregations can use the facilities when visiting the other communities. According to the researcher's findings, missionaries currently exchange services within their religious sect, limiting the exchange because the other missionaries in different denominations seldom have access to a different sect's facility.

Currently, in South Africa, there is a general directory of all the services provided by the Catholic Church called the Catholic Directory, and it is managed by the Southern African Catholic Bishops' Conference (SACBC, 2024). This platform is ideal and very helpful. It contains different Catholic universities, retreat and conference centres, dioceses, and offices in the Catholic Church. The directory provides all the information regarding a particular place, congregation, or parish. To the researcher's best knowledge, the only limitation of the Catholic directory is that it does not provide the user with much information about the travelling facilities when travelling to South Africa.

On the other hand, Eswatini has no such facilities besides the minimal diocese website. All departments of the church and missionaries' centres are independent. To the researcher's best knowledge, there is no platform available in South Africa nor in Eswatini that incorporates all the travelling logistics of missionaries into a single platform.

Presently, there are several service-based digital platforms available in the market. For example, Airbnb is one of the most popular service-based digital platforms providing different logistics facilities; the services extend beyond tourism lodging and include restaurant reservations and other excursions (Guttentag, 2019). However, many unique services provided by missionaries cannot easily be incorporated into such platforms. Similarly, well-known platforms such as Booking.com are ineffective for personalised missionary services.

Taking into account the aforementioned set of challenges, it is clear that there is a need to find new ways of integrating all missionary accommodation facilities into a single digital platform where missionaries can find all the facilities at the push of a

button, so to speak. This study is the first to explore ways to integrate a service-based digital platform for missionary activities that incorporate missionary services. The results of this study will be showcased in a travel-logistics system.

2.2. Digital Platforms

2.2.1. Digital platforms definition

According to Rohm, Kashyap, Brashear and Milne (2004, p.2), a digital platform is “an inter-organizational information system through which multiple buyers and sellers interact electronically to identify potential trading partners, select them and execute transactions”. These internet-based aggregators of buyers and sellers are known as B2B digital platforms. They operate as middlemen, facilitating transactions between the parties involved and allowing for the flow of value and knowledge (Reuver, Sørensen and Basole, 2018).

2.2.2. Service-based digital platforms

The rise of digital platforms has changed how companies operate. Digital platforms have grown in popularity and use in business-to-business (B2B) marketplaces, piquing academics' curiosity. Despite the growing attention, the area lacks a systematic method to fill the gaps left behind. With the rise of digital platforms, B2B connections are changing dramatically. Potential buyers and sellers are connected through digital platforms which allow them to negotiate and complete transactions (Chakravarty, Kumar and Grewal, 2014). Digital platforms are becoming more critical to coordinating economic activities and creating new value-generation and exchange models (Goyal and Kumar, 2021). They have contributed to constructing large-scale, efficient markets by bringing suppliers, buyers, and service providers together, forming their communities (Kalia and Paul, 2021).

There are several options that business organisations can use to adopt digital platforms. One option can be through an external interchange, which functions as an impartial platform where a service provider links business dealers. Another option can be a market-sponsored marketplace, which is created by a group of business dealers within a particular industry. Lastly, there is the private e-market, which is set up by either a seller or buyer for their own benefit (Truong, Le, Senecal and Rao, 2021).

Academic research interest in this topic is expanding with the increasing prominence of digital platforms in commercial practice. Researchers have generated a large amount of information in this sector, including theoretical insights ranging from digital platform adoption to performance results and platform management solutions (Shree, Kumar Singh, Paul, Hao and Xu, 2021). Nevertheless, little research has been done on securing such information, which we will focus on in the current study.

2.2.3. Existing travel-logistics digital platforms

Digitisation has reduced the distance between places and people, and the travel industry has significantly benefited from this revolutionary technology (Nishant, 2019). Digital platforms are quickly disrupting the industry. They provide travellers with global access and cutting-edge marketing and quality control tools. Customers have more options and better choices, on the one hand, and on the other, service providers have more prospects to engage and identify their target audience. Travel has not only become more accessible but also more readily available for people since the advent of digitalisation. Since the case study of the current study is a digital platform providing similar services, this section highlights a few existing travel logistics platforms that have facilitated the travel and the tourism industry to find how our proposed digital platform can best fit in or be improved from the existing one.

2.2.3.1. Booking.com

Booking.com, established in 1996, is a traveller and industry favourite, distinguished for three main reasons. The first is its complete scope: The website lists over 28 million different kinds of lodgings, varying from hotels, hostels, and B&Bs to holiday homes and luxury resorts. This means that when looking for a hotel by destination, Booking.com caters to more preferences than any other online travel agency (OTA). Second, the website is cost-effective, with pricing for flights and accommodations often being offered at diminished rates (Macdonald, 2021).

Finally, besides the standard services provided by most OTAs, Booking.com provides numerous luxuries by handling every part of a vacation, including tours, activities, and cabs to and from the airport. The user interface is also straightforward to utilise. On the home page, input the preferred destination and dates to choose a hotel. Then, narrow down the results to find the ideal match using the numerous filters available.

Users can also browse portfolios organised by destination or property type to find a specific hotel or get inspiration. Flights, car rentals, and other alternatives all have straightforward tabs (Robert, 2021).

2.2.3.2. Airbnb

Airbnb is a digital platform that enables individuals to rent out their extra rooms to travellers. These rental spaces are often entire homes (such as houses, condos, etc.) or private rooms in residences where the host lives (Guttentag, 2019). Airbnb's variety of offerings also includes some unique and unusual places to stay, like castles, igloos, treehouses, and more. The accommodations on Airbnb range from affordable to highly luxurious. Booking an Airbnb is quite similar to booking through online travel agencies like Expedia. However, the reservation process might involve direct communication with the host. The Airbnb platform empowers hosts to act as lodging providers by listing and managing their properties, showcasing them with descriptions and photos, engaging with possible visitors, and handling bookings and transactions from all over the world.

Airbnb promotes public reviews between hosts and guests, which helps to build the trust that is necessary for the platform to succeed (Jøsang, Ismail and Boyd, 2007). Airbnb provides a number of identity verification methods, free liability insurance with "Host Protection Insurance," free coverage for property damage through the "Host Guarantee," and a "Guest Refund Policy" that addresses things like deceptive listing descriptions in an effort to further strengthen security and foster trust. In an effort to enhance and broaden its offerings, the Airbnb has also added a number of new features. Among them are "Instant Booking," which permits some reservations to be made without the host's prior consent; the "Superhost" badge, which is awarded to hosts who are exceptionally active and have received high ratings; a "For Work Trips" filter for listings that are appropriate for business travels; and the "Airbnb Plus" badge, which is awarded to premium listings that have been personally inspected by an Airbnb representative.

In addition, Airbnb has worked with a number of travels planning firms to streamline business travel (Griswold, 2016). Most recently, Airbnb and a real estate developer teamed to build apartment buildings that are only intended for renting through Airbnb (Quackenbush, 2017). Airbnb has extended beyond vacation rentals by offering

restaurant reservations and curated local experiences, including tours and excursions organised by local hosts.

2.2.3.3. Trip Advisor

TripAdvisor is the best website to find unbiased reviews of anything from hotels to restaurants to attractions. Reading about other people's experiences can help you book (or not book) with confidence. TripAdvisor also operates as a metasearch engine, providing third-party links that enable users to make bookings influenced by reviews without needing to visit another online travel agency (OTA). Users can reserve hotels, vacation homes, tours, dining reservations and tickets flights on TripAdvisor (Macdonald, 2021).

2.2.4. Service-based digital platforms data security raised issues

Service-based digital platforms face several security challenges that affect the CIA Triad. Some of the vulnerabilities are listed below:

1. Confidentiality: Confidentiality is the first step in securing information in a digital platform. It comprises Authentication, Authorisation and Accountability, known as the AAA (Andress, 2014). User data confidentiality may be exposed if the data is not adequately encrypted or if unauthorised users access the server. For example, by intercepting communication between the client and server, a hacker may be able to steal sensitive user information such as credit card numbers or personal identification information. Some of the cyber-attacks associated with confidentiality are as follows:

- Phishing is a kind of cybercrime in which the perpetrator deceives the victim into divulging private and sensitive information such as; bank account detail, usernames, passwords or credit card information (Shankar, Shetty and Nath, 2019).
- Password attacks are the process of guessing or cracking a password to obtain entry into a system. It can also be a method for recovering passwords from data stored in the system (Tasevski, 2019).
- A man-in-the-middle attack is a kind of an attack that occurs when an attacker covertly intercepts and potentially alters the communication between two

parties who mistakenly think they are interacting directly with one another (Mallik, 2018).

2. Integrity: If data stored on the server is not secured correctly, its integrity may be compromised. A hacker, for example, may be able to modify or delete data stored on the server, resulting in the loss of critical information or the corruption of the entire system. Some examples of vulnerabilities are as follows:

- Malware is any software that interferes with or abuses a system's regular operation (Deng, Guo, Shen, Cui and Ping, 2023). A digital platform's integrity can be jeopardised by malware when it modifies or deletes data, introduces malicious code, or makes unauthorised access possible.
- SQL injection attacks are a kind of attack where a perpetrator inserts malicious code into a database query to gain access to the platform's database, steal data, or even alter or remove reliable data kept in the application (Crespo-Martínez *et al.*, 2023).
- Data manipulation attacks are fraudulent online activity where a bad actor modifies valuable digital documents and important data rather than simply stealing them to harm the company and cause agony (Hasti, 2019).

3. Availability: The system's availability may be threatened if the server experiences downtime or cannot handle the volume of user requests. For example, if the server fails or becomes overburdened with requests, users may be unable to access the platform, resulting in lost revenue, decreased user satisfaction, and reputational damage.

- Denial-of-service (DoS) attacks are malevolent attempts to interrupt, degrade, or block access to an information resource for legitimate users (Qadir Mir, Ahmad Mir and Maqbool Beigh, 2018).
- Distributed denial-of-service (DDoS) attacks happen when a perpetrator attempts to prevent people who are authorized from accessing services. This can involve overwhelming a network by flooding it, reducing bandwidth for genuine users, restricting access to services, or disrupting a particular system or user (Lau, Rubin, Smith and Trajković, 2000).
- Ransomware attacks are a form of malicious software designed to enable various harmful activities, such as preventing access to private data until a

ransom payment is received (Beaman, Barkworth, Akande, Hakak and Khan, 2021).

2.3. Data Security Frameworks

2.3.1. Data security framework definition

Data security frameworks are comprehensive and systematic ways that organisations use to protect their digital platforms and sensitive data against cyber threats and unauthorised access, disclosure, or modification (Taherdoost, 2022). These frameworks include rules, procedures, technologies, and best practices designed expressly to safeguard digital platforms like web applications, databases, cloud services, and other online assets (Azmi, Tibben and Win, 2018). In this context, the primary purpose of data security frameworks is to ensure robust data security of digital information while limiting the risk of cyber-attacks and data breaches.

2.3.2. Overview of various data security frameworks

Cybersecurity has undergone constant growth, leading to several data security frameworks intended to address the constantly changing difficulties associated with protecting sensitive data. In this section of the literature review, an examination of well-known data security frameworks and models regularly applied in the field is provided within this changing landscape.

There are numerous cybersecurity frameworks already in place. ISO/IEC 27001: Information Security Management System (ISMS), NIST Cybersecurity Framework, CIS Controls, GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and PCI DSS (Payment Card Industry Data Security Standard) are just a few examples. These frameworks cover a wide range of cybersecurity issues and, curiously, they all adhere to the CIA Triad model's core principles, which prioritise data confidentiality, integrity, and availability (CIA). The CIA Triad is a core paradigm for assessing and improving data security across sectors and regulatory settings.

Additionally, several additional models, aside from the CIA Triad model, have a similar methodology, and each offers a different perspective on the field of data security. These models include, among others:

Parkerian Hexad: An extension of the CIA Triad, this model introduces three additional dimensions, namely possession, authenticity, and utility, thereby furnishing a more comprehensive framework for assessing security principles (Reid and Gilbert, 2010).

Brewer and Nash Model (The Bell-LaPadula Model): This model improves the data security principles by focusing on implementing obligatory access restrictions using security labels and levels to guarantee strict data confidentiality and controlled access (Roslan, Hamid and Shamala, 2018).

Zero Trust Model: Rooted in a paradigm of distrust, this model challenges conventional notions of trust by implementing stringent verification and access controls for users and systems, closely aligning with the CIA Triad's emphasis on data confidentiality and integrity (Shore, Zeadally and Keshariya, 2021).

The CIA Triad model is the recommended method for data security because of several important aspects. By consistently addressing confidentiality, integrity, and availability, it first and foremost presents a harmonised perspective (Baybulatov and Promyslov, 2020). This all-encompassing perspective ensures that data is protected from illegal access, alteration, and unavailability, smoothly integrating with the multifarious complexity of modern cybersecurity. The CIA Triad model is globally applicable across various businesses and sectors due to its simplicity and thoroughness (Samonas and Coss, 2014). Regardless of the size or scope of their organisations, businesses can use the concepts in this model as a starting point for developing their data security plans. This adaptability fosters a common understanding of security goals and speeds up the uniform application of security measures.

A search on the literature about the CIA trial model revealed that many scholars have used this model in their works. Table 2.1 below provides some examples of those scholars who have used the CIA trial model.

Table 2.1. Scholars utilising the CIA Triad in their work

	Author(s)	Summary
1)	Warkentin and Orgeron (2020)	In this paper, the authors explain how important it is to use the CIA Triad to ensure data security. The CIA model is employed using blockchain technology to insure non-repudiation of distributed ledger. The author highlights how using the CIA Triad can assist developing blockchain application.
2)	Halabi and Bellaiche (2018)	The CIA Triad model was utilised in this study to create a broker-based framework for handling Cloud Security-SLAs. The approach aided in quantifying and measuring cloud service security aspects (Confidentiality, Integrity, and Availability). This method allowed for a more impartial evaluation of cloud providers and promoted secure cloud adoption for enterprises that deal with sensitive data.
3)	Kebande et al. (2021)	The study suggests a Multi-Factor Authentication model (MFBC_eDS) for Internet-of-Vehicle (IoV) environments that is based on blockchain and has an embedded digital signature. The integration of SAML and SSO capabilities enhances authentication and defends against hostile assaults. In IoV and vehicular cloud applications, the concept improves security by striving to achieve the Confidentiality, Integrity, and Availability (CIA) Triad.
4)	Kumar, Saha, Rai and Kim (2018)	The research presents an end-to-end authentication mechanism to address security challenges in vehicular ad hoc networks (VANETs). It ensures the CIA Triad services for VANET connection by transmitting data in an encrypted manner. To avoid intrusion through downloaded data, a sandboxing mechanism is used. The simulation results indicate the effectiveness of the solution.

5)	Berghout, Benbouzid and Muyeen (2022)	In the paper, machine learning (ML) is used to analyse cyber-attacks in smart grids. It categorises cyberthreats based on the data security CIA Triad and examines difficulties, limitations, and potential future uses for ML cybersecurity in smart grids.
6)	Catak (2018)	The study discusses the classification of harmful network traffic aimed at the CIA Triad's accessibility. It provides a two-stage filtering strategy for network traffic identification and employs L1-norm based sparse linear models for feature selection to improve the classification model's predictive performance. The simulation results validate the effectiveness of the proposed method.
7)	Kang, Fahd and Venkatraman (2018)	The study presents a unique technique for detecting man-in-the-middle (MITM) attacks using a learning-based inferencing algorithm at a trustworthy time server (TTS). It provides a low-cost solution for addressing the constraints of conventional intrusion detection systems (IDS) while adhering to the CIA Triad principles.
8)	Bhattacharjya (2022)	The research looks towards using blockchain technology to overcome security issues in centralised IoT and CPS architectures. It explores the possible benefits of blockchain for sustaining the CIA Triad in these systems and proposes a decision support system (DSS) using a mathematical model for this purpose.
9)	Qammar, Ding and Ning (2021)	The study examines security and privacy breaches in federated learning (FL). It reviews recent studies on FL attack surfaces, classification, and defence strategies. It highlights the breach in the CIA security triad and offers FL models and privacy attack tools. The report also covers technological issues and future research directions for creating reliable FL systems.

10)	Li, Doh and Chae (2016)	The study presents a group authentication system based on Lagrange interpolation polynomial theory. It distributes secret shares among group members for subsequent authentication, with reduced computation and communication difficulties than existing systems. The system ensures the CIA Triad security model.
11)	Hartono, Kim, Na, Simpson and Berkowitz (2013)	The study looks at perceived site security in B2C e-commerce. It introduces a new second-order structure based on the CIA Triad model, which consists of Confidentiality, Integrity, and Availability. The findings indicate the superiority of this novel measure and validate its nomological validity.
12)	Baybulatov and Promyslov (2020)	The paper investigates cybersecurity evaluation in control systems using the traditional CIA triangle approach (Confidentiality, Integrity, and Availability). It highlights availability as the crucial characteristic and suggests utilising delay as a sign of cybersecurity. For a variety of system situations, the study uses network calculus to estimate latency based on backlog bound and service curve frameworks.
13)	Gonzalez, Gronsund, Dimitriadis and Reshytnik (2021)	The paper examines 5G network security implementation, utilising the CIA Triad model to define policies for availability, confidentiality, and integrity. It focuses on the 5G-VINNI Norway facility and the services it offers 5G-verticals.
14)	Baars and Spruit (2012)	This study introduces the Secure Cloud Architecture (SeCA) paradigm, which is based on data classifications and cloud environment testing utilising the CIA Triad framework. Through the integration of the CI3A extension and eight other factors, the model assures a secure cloud architecture. The use of the

		SeCA model is shown throu(Saleem <i>et al.</i> , 2022)tances.
15)	Saleem et al. (2022)	The study introduces ProofChain, a blockchain-based decentralised PKI system. By doing this, confidence among decentralised Certificate Authorities (CAs) is maintained and dependency on centralised CAs is removed. ProofChain has been tested against the CIA Triad model, is compliant with PKI standards (X.509), and has been shown in real-world scenarios on the Ethereum network's private testbed.

2.4. Blockchain Technology

2.4.1. Blockchain technology definition

Blockchain is a distributed technology based on peer-to-peer network principles and cryptographic primitives like asymmetric encryption and digital signatures (Balaskas and Franqueira, 2018). It allows users to share information and record transactions without interference and coordination. Blockchain systems use a secure database, based on a consensus protocol to determine which valid data gets added to the network. This ensures that information is distributed and shared across the participant's network (Balaskas and Franqueira, 2018).

Blockchain technology is currently regarded as the most revolutionary technological innovation of the fourth industrial revolution. Blockchain technology can completely transform the economy through top-notch efficiency. This is possible because it is designed to store transactional data. Besides, blockchain is a natural fit for large systems such as e-commerce and service-based digital platforms (Mohammed *et al.*, 2021). In more technical terms, blockchain is a method of keeping and transacting systematically structured records. It is universally used in businesses, education, healthcare, digital marketing, retail, and information technology sectors. Blockchain enables all industries to track the evolution of systems and transactions stored across all network resources. It offers integration, increased efficiency, privacy, security, and other opportunities, particularly in its significant technological advancements (Quluzada and Maharramli, 2019).

A record of all past transactions executed within the system is stored by every participant (stakeholder) on the blockchain. However, no single party or node owns the system, signifying its decentralised structure. Since every action is transparent and can be audited by all participants, this decentralised system fosters trust. For a transaction to proceed, a consensus algorithm must be followed, meaning that nodes need to reach agreement for validation and authorisation. Moreover, blockchain-based systems eliminate the need for mediators or third parties in transactions, which lowers transaction costs. These transactions are also irreversible, removing the necessity for any public or private institution to serve as an intermediary, making the system more efficient. The participants involved in the transaction don't need to trust one another,

because the underlying code and system are error-free. The three most common definitions of blockchain are as follows (Yadav and Singh, 2019):

- From a technical perspective, it is a back-end database that manages a distributed ledger, which can be publicly inspected.
- In a business context, it is an exchange network that facilitates the transfer of value, assets, and transactions between peers without the intervention of intermediates.
- From a legal standpoint, it verifies the history of transactions, effectively replacing previously trusted entities.

2.4.2. Blockchain classification

Blockchains are classified as Public, Consortium, and Private based on users' participation, and main and side chains based on chain relationships. Also, numerous blockchains can work together to form a network, where the chains are interconnected to create an Interchain (Wang et al., 2019).

- a) **Public Blockchain:** A Blockchain consensus that everyone may access. They may send and validate transactions within the blockchain topology. Everyone can compete for billing rights. These blockchains are normally considered "completely decentralised," similar to the Bitcoin Blockchain, in which the information is fully revealed.
- b) **Private Blockchain:** A blockchain in which a single organisation retains the right to write. Reading permission may be public or somewhat restricted. Additional company options exist, such as database management, audit, and so forth. Public access is not required in most cases.
- c) **Consortium Blockchain:** A blockchain whose consensus process is controlled by pre-selected nodes and is located between the Public Chain and the Private Chain. For example, consider a system of 15 financial institutions, each of which manages one node and at least 10 of which must confirm each block in order for it to be recognised as valid and added to the chain. The ability to read the blockchain can be granted to the general public, limited to participants, or "hybrid". Such chains are referred to as "partially decentralised".

2.4.3. Blockchain technology architecture

A blockchain, in theory, should be viewed as a distributed append-only time-stamped data structure. Blockchain technology enables the creation of a decentralised peer-to-peer network in which non-trusting participants can transact in a verifiable manner without the need for a trusted authority. To accomplish this, consider blockchain as a collection of interconnected mechanisms that provide specific features to the infrastructure, as shown in Figure 2.1. The fundamental units of this system are peer-to-peer transactions, which signify agreements between two people and can involve the exchange of digital or physical assets, the accomplishment of tasks, or other similar activities. This transaction is signed by at least one participant and distributed to its neighbours. An entity that is connected to the blockchain is called a node. Full nodes are those that verify every rule in the blockchain, group transactions into blocks, and decide which ones should be accepted and recorded on the blockchain and which ones should be refused (Casino, Dasaklis and Patsakis, 2019).

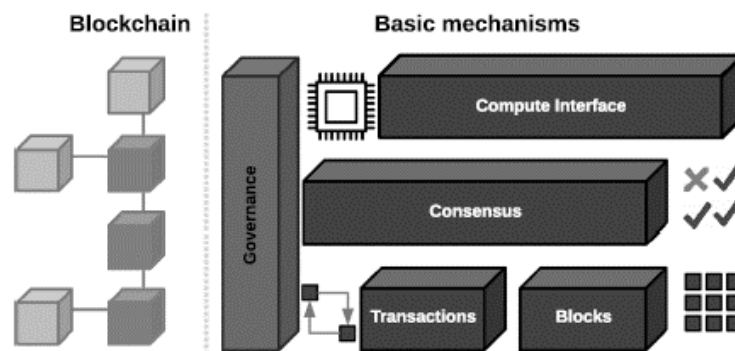


Figure 2.1. An overview of blockchain architecture (Casino et al., 2019)

2.4.4. Application of blockchain technology

Blockchain has been implemented in different fields, such as health, education, and cryptocurrency. Blockchain has distinct traditions in the health sector, such as patient records, medical reports, strategies, and many more. Data from various sources are collected at multiple frequencies and terms for observation and analysis (Azaria, Ekblaw, Vieira and Lippman, 2016). To analyse this data, hospitals require efficient research tools. It has also been observed that they sometimes require confidential and secure data in the medical field. For this purpose, blockchain technology is used in this sector to make data more secure and accessible to hospital staff and minimise any alterations by other users (Esposito, De Santis, Tortora, Chang and Choo, 2018).

Medical information records are critical, hence the need for solid security and management (Aslam, Manzoor and Babar, 2019).

In education, blockchain is the only link evidence of digital events that create a duplicate on each network node. The entire record is distributed across node networks. It stores the completion of academic credits, often referred to as degree certificates. Each time a student earns a degree certificate, the blockchain gains a new block, which can be accessed by authorised industry professionals. Students can also share this information with prominent companies and include it on their CVs. Blockchain technology ensures that a publicly awarded degree from a university is validated and authorised (Aslam *et al.*, 2019).

There are numerous cryptocurrencies globally, but the most notable are Bitcoin and Ethereum (Miraz and Ali, 2018). Cryptocurrency functions as a traditional currency, allowing users to purchase goods and services efficiently. People are beginning to trade cryptocurrency and save their assets using this technology, which is now considered a well-established business. Cryptocurrencies are exchange transactions that are created and stored within a blockchain. These transactions are highly secure due to encryption and decryption methods used to verify monetary units and record all transactions securely. Cryptocurrencies do not exist in a physical form but are only available through blockchain networks (Aslam *et al.*, 2019). Cryptocurrency is not controlled or centrally controlled; however, it is managed because the blockchain network is overly decentralised. The other block must verify its validity when any transaction is performed in a chain. After verification, a new block is formed the chain, and the transaction record is stored in it. Each new block is identified through a hash generated by a proof-of-work process (Li, Jiang, Chen, Luo and Wen, 2020). Cryptocurrency has numerous benefits, increasing the transparency of every permanently recorded transaction that everyone can view and observe (Eyal, 2017). No one can send back their transaction because of the good block and previous hash, also known as a forward transaction (Aslam *et al.*, 2019).

2.4.5. Existing blockchain frameworks

The blockchain framework is a set of software tools that simplify designing and deploying blockchain applications with minimal customisation (Quasim, Khan, Algarni, Alharthy and Alshmrani, 2020). Because of all of these advantages, blockchain frameworks are well-known among experts. Blockchain frameworks are essential for developing blockchain-based applications (Maria, 2021). There are numerous blockchain-based platforms available on the internet today. Even though each venue is based on the same blockchain-based technology, each forum is unique. The following section will discuss two of the most popular enterprise frameworks for implementing blockchain solutions.

2.4.5.1. The Bitcoin overview

Bitcoin is a blockchain-based distributed protocol developed by Nakamoto that facilitates payments and transfers of cryptocurrency among participating entities (Monti and Rasmussen, 2017). There is no need for a centralised bank to manage balances, oversee monetary transactions, or issue new currency. A globally distributed transaction leader is maintained in the Bitcoins network. Each transaction represents the transfer of payment from one node to another. The payment address is generated using a sequence of cryptographic hash functions linked to the sender's public key, and every new valid block is disseminated to every node on the network. Currently, Bitcoin uses the SHA-256 algorithm for its hashing processes (Balaskas and Franqueira, 2018).

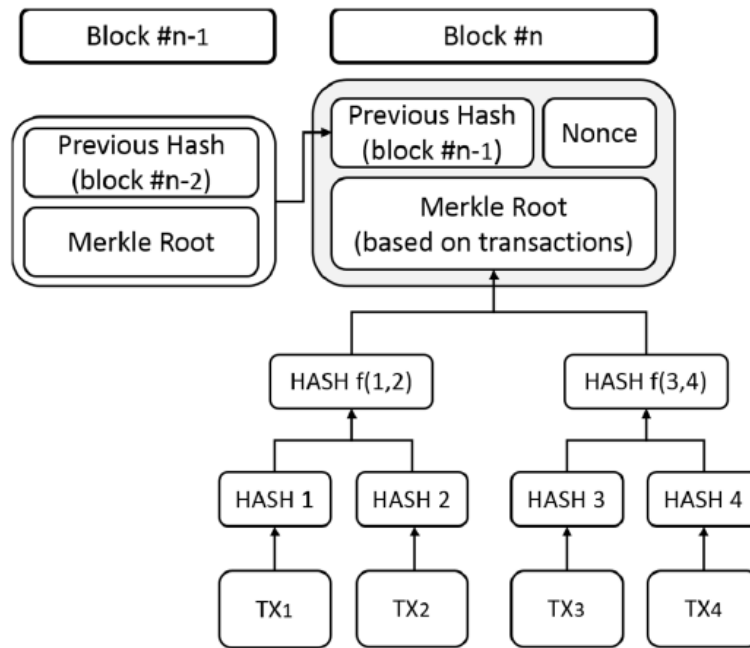


Figure 2.2 Bitcoin block construction using the Merkle Tree (Balaskas and Franqueira, 2018)

Miners have verified the transactions listed in a new block and ensured that no currency is spent more than once. The transactions of a new block are consolidated into a single hash, acting as the Merkle Tree root. Transactions are only found in the leaves of a binary tree structure. The hashing scheme shown in Figure 2.2 propagates and combines transaction hashes until a single hash is acquired and added to a new block as the Merkle Root of transactions in the block. The new block additionally contains the prior block's hash; this, along with the hashing and the duplication of the ledger (shared among network participants), makes blockchain technology tamper-resistant. If two miners broadcast a new block and one of them is a subset of the other, the block with the higher number of transactions is retained (Balaskas and Franqueira, 2018).

2.4.5.2. Overview of Ethereum

Ethereum is a public, an open-source, distributed blockchain computing platform with smart contract features. It extends Bitcoin and makes use of virtual machine technologies (Ethereum Virtual Machine) to enable custom business logic, in other words, smart contracts, to be employed in new applications. The primary platform is a public network from which anyone can download applications to run on their machine (Pongnumkul, Siripanpornchana and Thajchayapong, 2017). This technology also serves as the basis for Ether, a related form of cryptocurrency. Ethereum offers a

Turing-complete programming language for developing smart contracts, allowing for the creation and execution of programs directly on the blockchain (Ferretti and D'Angelo, 2020).

Ethereum runs based on accounts and their balances, which change as a result of state transitions. The state displays all account current balances, along with any other pertinent data. The state is encoded and kept up to date via a different data structure called a Merkle Patricia tree rather than being directly saved on the blockchain. To maintain anonymity, Ethereum accounts are pseudonymous and connected to one or more addresses, just as previous permissionless blockchains (Garcia-Alfaro *et al.*, 2015).

For the aim of this study, Ethereum was selected as the blockchain framework because, in some respects, the Ethereum blockchain framework is unique from other blockchain frameworks. First, Ethereum is a permissionless, public blockchain that uses the digital money Ether and Turing-complete smart contracts for complex distributed applications (Aldweesh, Alharby, Mehrnezhad and van Moorsel, 2021). Second, Ethereum has demonstrated its adaptability in several applications, including smart grids and the administration of healthcare data (D. Lalitha Bhaskari, 2021; Wen, Fang, Wu and Zheng, 2021). Ethereum provides strong, smart contract capabilities, a vibrant developer community, and adaptability for creating decentralised applications (Argañaraz, Berón, Pereira and Henriques, 2020; Bistarelli *et al.*, 2020). As a result, Ethereum proves to be suitable for our research goals. The rationale for this choice is further supported by its extraordinary versatility, wide adoption, and innate ability to successfully cater to our investigation's particular scope, which is to develop a secured service-based digital platform.

2.4.6. Blockchain technology for data security for digital platforms

According to Raturi (2020), blockchain is one of the best technologies for data protection. Rapid innovations in digital technology have also introduced new data security challenges. Organisations need to use advanced cryptography-based vaulting techniques and strong authentication systems to protect their data (Raturi, 2020). Blockchain technology can now protect against damaging cyberattacks and solve the issue of data security. According to reports, the global market for blockchain technology is expected to grow to a value of almost \$20 billion by 2024 (Raturi, 2020).

Blockchain technology has seen adoption across various sectors, with the financial industry being the most prominent through the use of cryptocurrencies. However, its application extends to cybersecurity as well. Mathew (2019) conducted a study on how blockchain could be used to develop tools that combat fraud and identity theft. Users face constant threats from unauthorised access and data modification, primarily due to the centralised nature of data storage. This centralisation allows hackers to target a single location and alter data with malicious intent. By contrast, blockchain's decentralised storage system prevents such risks. Sensitive information can be distributed across millions of computers, each holding a copy of the data. If a few systems are compromised, the integrity of the overall data remains intact unless a large number of copies are infiltrated. Blockchain platforms are also gaining significant traction in business and software architecture.

Platforms are progressively becoming key characteristics of the digital world, whether in the commercial, government, hospitality, or health sectors. They are crucial to digital ecosystems (Troup, 2017). This growth in digital platforms has resulted in the rise of cybersecurity; companies face high risks in the digital economy. Companies need to maintain vigilance by scaling up their security protocols to meet the threat (Schlesinger, 2020). This growth of online cybersecurity instability has resulted in much research on how cybersecurity can best help resolve the challenge. Having discussed the escalating cybersecurity concerns, the need for enhanced security protocols, and how blockchain is used for data security based on previous literature, we now turn our attention to the different mechanisms used to develop secured digital using blockchain technology as a reliable and innovative solution to ensure data security in the digital world.

2.4.7. Blockchain technology to guarantee data security

Based on the issue raised earlier, this section provides a solution using blockchain technology by following the principle of the CIA Triad.

2.4.7.1. Confidentiality

Following are some ways that blockchain technology can promote confidentiality:

- **Authentication**

Based on previous studies, it has been demonstrated that blockchain can guarantee a secured authentication of users online. Their publication (Zheng, Xie, Dai, Chen and Wang, 2018) confirms that blockchain technology makes identity verification possible thanks to a decentralised network of nodes, ensuring that only authorised individuals can access sensitive data. Another study (Underwood, 2016) stipulates that smart contracts can enforce access controls on a blockchain network to guarantee that only authorised parties have access to sensitive information. These are some examples of publications that have affirmed this. This work demonstrates it through a prototype that was developed and tested.

- **Authorisation**

Blockchain guarantees authorisation by establishing fine-grained access restrictions that allow authorised parties to access sensitive data (Zheng et al., 2018). Authorisation can also be implemented through encryption. Blockchain technology can help safeguard the privacy of data stored on the network to allow only permitted users to access it (Gad, Mosa, Abualigah and Abohany, 2022).

- **Accountability or Audit**

Blockchain technology offers an auditable, transparent, and unchangeable ledger that may be used to check that access to sensitive information complies with rules and policies (Zheng et al., 2018). It also allows for data access and alteration tracking, which can be used to spot attempts at unwanted access (Gad et al., 2022).

To guarantee the confidentiality of information on a digital platform, based on the studies that have been done before, all these elements (Authentication, Authorisation and Accountability) combined, blockchain technology can offer a secure and confidential platform immune to numerous cyber-attacks that can compromise the confidentiality of digital platforms. By combining these properties, blockchain technology can offer a safe and robust platform resistant to various cyber threats that can damage digital platforms.

2.4.7.2. Integrity

Data integrity can be guaranteed on a digital platform through immutability offered by blockchain technology through an unalterable ledger that can stop data from being changed or deleted without permission. Secondly, integrity is guaranteed through the blockchain's distributed consensus process that guarantees non-repudiation of data since it allows data to be stored correctly and consistently (Mougayar and Vitalik Buterin, 2016).

2.4.7.3. Availability

Blockchain technology enables decentralised data processing and storage, making the platform more resistant to DoS and DDoS attacks (Tapscott and Tapscott, 2018). Availability is also guaranteed through the fault-tolerant nature of blockchain technology, which guarantees that the platform can continue functioning even if some nodes are not on the network (Nakamoto, 2008).

The combination of Confidentiality, Integrity, and Availability offered by blockchain technology provides a robust and secure platform that can withstand various cyber threats. Blockchain emerges as a game-changing answer to the urgent data security problem by abiding with the CIA Triad's model. The following section will examine the technical and practical features of the blockchain system and give a detailed examination of its mechanisms and uses.

2.4.8. Blockchain technology for developing secured digital platforms

This section thoroughly explores how blockchain technology can be used to create secured service-based digital platforms. This section explores the detailed mechanisms that provide blockchain's robust security infrastructure, building on the fundamental ideas covered in the other sections. This discussion attempts to clarify how this new technology is set up and used to guarantee security in service-based digital platforms.

2.4.8.1. Ethereum

As mentioned earlier Ethereum is the chosen framework used for the purpose of this study. Like Bitcoin, Ethereum is a public blockchain employs the Proof of Work (PoW) consensus mechanisms (Gavin Wood, 2014). The PoW algorithm is a method

employed by blockchain networks to select block creators from a pool of untrusted participants. Miners compete with one another in this process to find a hash value that satisfies the necessary requirements. In a public blockchain, this system introduces the concept of a cryptocurrency economy, rewarding the successful miner with bitcoin for achieving consensus. The integrity of previous blocks is maintained by linking newly generated blocks to the preceding ones through the “previous block hash” stored within the header of the block, before being distributed to users across the blockchain network. This decentralised system operates without central administrators, with all blocks and transactions fully accessible to the public.

Ethereum enables the development and implementation of smart contracts which are used to develop decentralised apps (Szabo, 2018). Smart contracts are written in Solidity, a Turing-complete language, stored on a distributed database, ensuring the accuracy of results based on automated execution and input (Christidis and Devetsikiotis, 2016). The operation of smart contracts in Ethereum is depicted in Figure 2.3. An Ethereum Virtual Machine (EVM) bytecode that has been created using Solidity is compiled and stored on the ledger. Within the EVM environment, this code is executed by Ethereum clients such as Geth (Go-Ethereum).

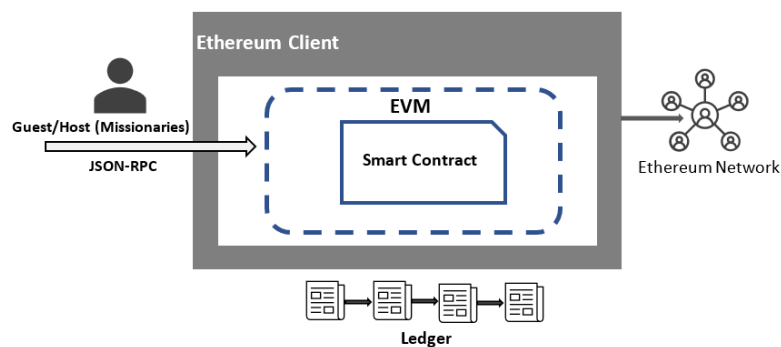


Figure 2.3. Ethereum framework architecture

- **Ethereum blockchain technology to guarantee data security**

Blockchain employs what is known as building blocks, which are made up of three components.

- 1 **Cryptography and encryption:** These offer essential security defences such as privacy, authenticity, non-repudiation, and authorisation (Omolara and Jantan, 2019; Omolara, Jantan, Abiodun, Arshad and Mohamed, 2019).

- 2 **Consensus mechanisms:** It is these algorithms decide if a fresh block of confirmed transactions should be accepted into the chain (Omolara and Jantan, 2019).
- 3 **Hashing and timestamp of the preceding block:** Data integrity is guaranteed in this way. The blockchain structure makes it easier to trace back to a specific transaction because of the constant and unchangeable data provenance it provides (Omolara *et al.*, 2019).

In Figure 2.4, the three main components of a blockchain are shown.

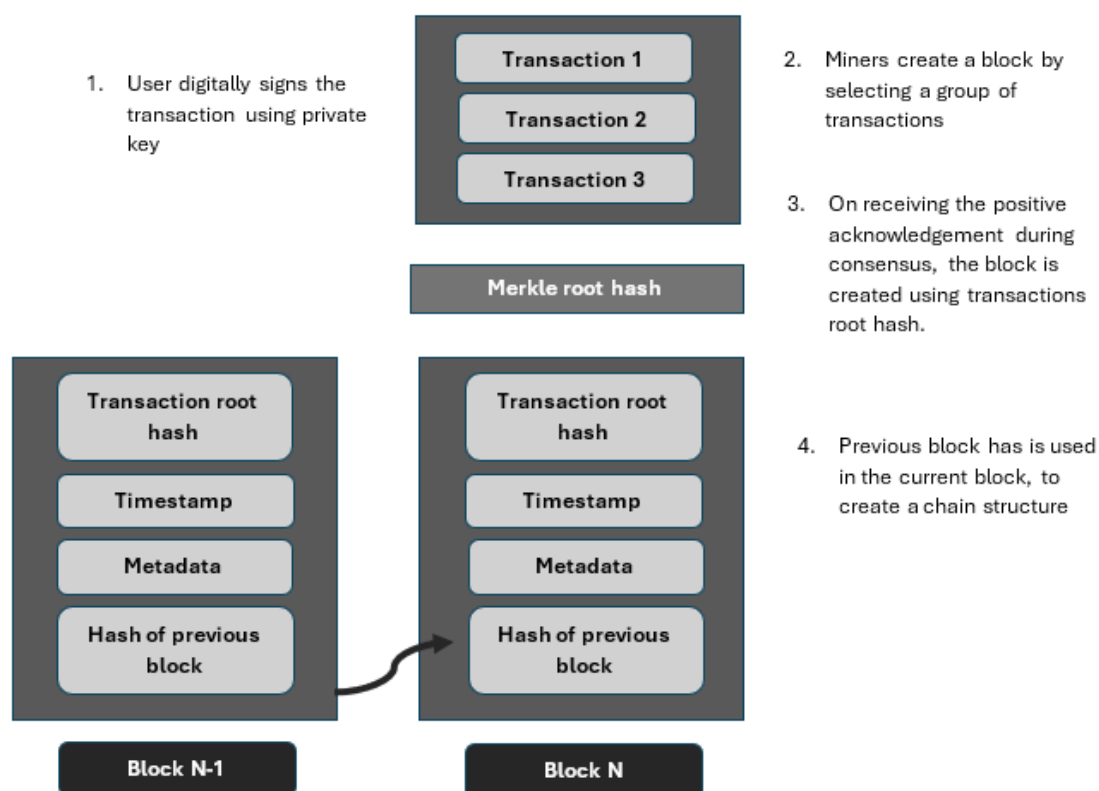


Figure 2.4. Building blocks of a blockchain

Blockchain technology utilises a linked-list data structure. The blockchain's participant nodes validate transactions (Kang *et al.*, 2017). Every block is hashed to preserve confidentiality and includes a collection of legitimate transactions. Each block creates a blockchain that works like a linked list by storing the hash of the previous block. All confirmed transactions are tracked by each block. The hash value is greatly impacted by any attempt on the part of a hacker to change the contents. All other nodes in the network must agree before a new block can be added to the chain, guaranteeing the

legitimacy of each block (Tosh, Shetty, Foytik, Kamhoua and Njilla, 2018). This is illustrated in Figure 2.5.

Below is a discussion of the two main responsibilities of any blockchain member:

- **Start transaction:** A transaction must be initiated by the participant for the blockchain to be active or initiated. Other participants in the network then verify the transaction.
- **Act as miners:** In order to compete to add a block, broadcast new blocks, validate transactions, and verify transactions, participants can assume the role of miners.

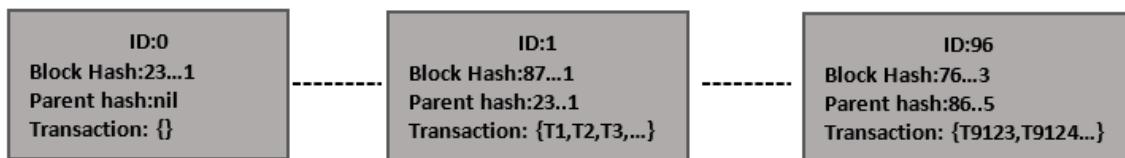


Figure 2.5. Blockchain example

- **Consensus mechanism**

The decision-making process used to decide whether to add fresh, verified, or legitimate blocks to the blockchain and improve trust is known as the consensus mechanism. The two consensus methods that are most frequently utilised are Proof of Stake (PoS) and Proof of Work (PoW) (Bina, 2017) .

- Proof of work:** This method uses the gossip protocol to disseminate any new transaction on the blockchain network to every node on the network. To build a block, a group of transactions is chosen by miner nodes. The nonce and each chosen transaction are hashed and validated. The hashing procedure is iterated using distinct nonces until the targeted level of difficulty is attained. A block is transmitted to every other node after it is produced. Next, each node uses the supplied nonce to confirm the block. The block is added to the chain and the miner who successfully makes it and receives consensus from the network is rewarded (Bina, 2017). When two miners generate a block at the same time, the network receives both blocks, creating two distinct branches. One branch will be retained and the other eliminated as the chain grows depending on where the next block is inserted. Many other platforms, including Ethereum and Bitcoin, presently use this proof of work consensus technique.

b) Proof of stake (PoS): The proof of work mechanism demands substantial computational power to generate a block that meets the required difficulty level, often resulting in the miner with the greatest computing resources being the winner. To overcome this limitation, the proof of stake mechanism was developed. Miners, also known as validators, are required by this system to stake, or deposit, a predetermined quantity of coins into the network. Next, a pseudorandom order is used to choose validators. The validator is in charge of confirming transactions and starting a new block after they are chosen. Subsequently, additional nodes receive this block and broadcast it to them, asking them to confirm its legitimacy and offer a positive consensus (Bina, 2017).

2.4.8.2. Decentralised application development technology

DApp refers to the idea that management and control of applications are dispersed over several nodes or entities rather than being centralised in one place (Steinheimer, Trick, Fuhrmann, Ghita and Frick, 2017). DApps are built on the blockchain that uses smart contracts to speed up transactions and enable peer-to-peer communication (Schäffer, di Angelo and Salzer, 2019). They resist security problems like hacking attempts and data breaches since they run on a distributed network (Chen, Pendleton, Njilla and Xu, 2019). The essential tools required to assist the building of DApps are described in this section. The potential benefits of decentralisation, transparency, and security, which the realm of blockchain technology naturally offers, can be explored by developers with the help of these crucial tools.

a) MetaMask

MetaMask is essential for developing and testing smart contracts (Pramulia and Anggoroajati, 2020). The user's private key is kept in the blockchain wallet, which also keeps track of the account's balance and makes and submits transactions to the network on the user's behalf. Wallets are the most accessible way to use blockchain in this sense. To make it simple to utilise in a PC or mobile device, this study makes use of MetaMask, the most well-known browser extension for an Ethereum wallet. Chrome, Firefox, Opera, and other browsers presently support it, and a mobile beta test is in progress. It enables users to create transactions, establish digital signatures,

and administer their Ethereum accounts. Users may simply access the blockchain's smart contract thanks to MetaMask.

b) Solidity

Solidity is a programming language focused on object orientation, designed specifically for building smart contracts on the Ethereum platform. It merges features from both JavaScript and Java (Mohanty, 2018a). Developers can incorporate business logic, enforce constraints, and set rules into the smart contract by utilising Solidity. After it is put into effect, a smart contract is a formal agreement between the parties involved, and all nodes in the blockchain network are required to abide by it.

c) ReactJS

Among front-end frameworks, Angular, Vue.js, and ReactJS are prominent. Angular is robust and suitable for large-scale applications due to its two-way data binding and dependency injection but can be less efficient for dynamic rendering (Mohit, 2023). Vue.js, while lightweight and fast for smaller projects, lacks the scalability needed for complex applications (Abhimanyu, 2024). ReactJS, with its virtual DOM and component-based structure, ensures high performance and efficient updates, making it ideal for dynamic and interactive platforms (Gurneet Kaur, 2024). This combination of performance and flexibility makes ReactJS the most appropriate choice for this study.

d) Hardhat

Hardhat is a popular tool for testing DApps (Mohanty, 2018b). It utilises dynamic testing methods such as property-based and model-based testing to thoroughly test and analyse the source code of smart contracts (Min, Lee and Lee, 2019). It has been evaluated among the top 100 most popular DApps and has shown high precision in identifying vulnerabilities (Skowroński and Brzeziński, 2022). Therefore, Hardhat is a reliable tool for testing DApps and ensuring their security and functionality.

e) IPFS

A centralised system is usually run by one business, therefore in order to access the data, users must rely on this company. The interplanetary file system (IPFS) can be used to lessen this reliance. Similar to BitTorrent, IPFS enables the complete

dissemination of web apps. Rather than using location-based addressing, it makes use of content-based addressing. Unlike location-based addressing, which requires users to specify the IP address or domain name from which the content will be obtained, content-based addressing just requires users to identify the specific content they desire. Content within IPFS can be identified by hashing, which keeps it safe from manipulation (Gregory, 2023).

Figure 2.6 shows the construction of the IPFS file system. Up to 256 KB of data can be stored in each IPFS object. If the size is exceeded, a new empty IPFS object is generated with a connection to a different portion of the data, and the data can be divided up and stored in other IPFS objects. IPFS uses a Merkle tree structure to store data. Once data is stored, it cannot be altered, just like the blockchain.

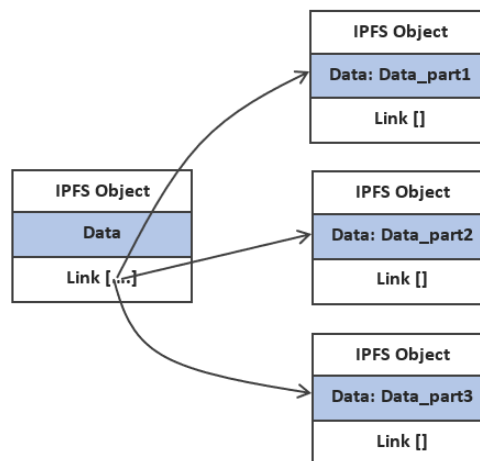


Figure 2.6. IPFS Structure

f) Fleek network

The decentralised edge platform Fleek Network is designed to make it easier to install and manage effective web services (such as CDNs and serverless operations) (Fleek Network, 2023). Developers can easily design and use a wide range of edge services thanks to the globally distributed and autonomously controlled network of edge nodes provided by Fleek Network. These services receive economically and cryptographically protected infrastructure, node and geographic coverage assurances, stable and predictable pricing, and uniform quality and performance across all services offered on the network.

2.5. Related work

There have been numerous studies to investigate the application of blockchain technology for data security in the digital platform. This section reviews recent literature on this topic, starting from the history, the application, and the current stage of the study and what needs to be improved.

Chatterjee and Chatterjee (2018) provide details, history, and evolution of blockchain and some insight into its revolutionary impact on Information Technology (IT) and non-IT industries. The objective was to comprehend the fundamentals of blockchain technology and its wider applications. According to their research, blockchain technology is a foundational tool that has the ability to impact a wide range of industries through safe and decentralised digital transactions. A literature review was conducted by Seebacher and Schüritz (2017) to explain the impact and concept of blockchain technology. Their goal was to gain a complete understanding of how blockchain is transforming diverse domains, providing insights into its transformative potential. The review's findings demonstrate blockchain's diverse influence across sectors, which advances the understanding of its conceptual foundation and practical ramifications. According to one source (Nofer, Gomber, Hinz and Schiereck, 2017), the authors explained blockchain technology more theoretically using examples and applications. The purpose was to contribute to the theoretical understanding of blockchain's potential applications.

Prior research (Rossi, Mueller-Bloch, Thatcher and Beck, 2019) expanded on using blockchain technology in the financial sector. The study gathers some of the papers that conclude the impact of this booming technology on business and information systems. The research aimed to understand how blockchain is specifically influencing financial processes. In addition, researchers (Zutshi, Grilo and Nodehi, 2021) conducted a study to clarify the value proposition provided by blockchain technology. Their research revealed that by offering extra data security, authenticity, and traceability features, blockchain technologies can support identification and user management forms including biometrics, password systems, and Authenticator Apps. User management is critical for any digital platform because maintaining trustworthy identities and permissions is the foundation for establishing trust in the system (Yang, Yi, Nepal, Kelarev and Han, 2020). User managements consist of several

components, including identity, privacy, permission, activity logs, and profile, which many authors have discussed in the literature.

In terms of identity, by assigning everything a digital identity, spreading storage rather than centralising it, and automating operations with smart contracts, blockchain's unique technology has the potential to bring transparency and trust to the digital ecosystem. As a result, the concept of "decentralised digital identity" is an essential aspect of a blockchain network, and it may even be the starting point (Aydar, Ayvaz and Cetin, 2019). Blockchain's inherent properties prevent tampering with these IDs and allow for process digitization. To further secure user privacy, the identity management blockchain can be separated from other services platforms.

Furthermore, in order to authenticate the identity of each wallet holder, the majority of blockchains give them access to a Private and Public Key. For any kind of activity or transaction, the Private Key is necessary. But this is often at the heart of technology, and when more sophisticated and intuitive solutions become available, the end-user won't have to remember and enter private keys. To enhance this, there's the usage of ID systems, biometrics, Google authenticators, and seed words (Zutshi *et al.*, 2021). A recent study (Hou, 2017) concluded that using blockchain to create identities can drastically cut bureaucracy while improving security, efficiency, and openness in government activities, allowing individuals to access their records and personal information using the blockchain-based public services platform.

A series of recent studies have highlighted the potential of blockchain technology in enhancing privacy protection. de Haro-Olmo, Varela-Vaca and Álvarez-Bermejo (2020) underscore the importance of blockchain in safeguarding privacy, particularly in payment transactions, electronic voting, and data sharing. Junejo, Hashmani and Memon (2021) further emphasise the need for a comprehensive evaluation framework to assess the efficiency of blockchain privacy solutions, while Wang, Zhao and Wang (2020) survey existing privacy protection technologies and proposes future research challenges in this area. These studies collectively underscore the significant role of blockchain in privacy protection and the need for further research in this domain.

A range of studies have explored the potential of blockchain technology for permission management. Monrat, Schelen and Andersson (2020) and Kakarlapudi and Mahmoud (2021) both highlight the importance of permissioned blockchain platforms in ensuring

data privacy and security. Monrat's performance evaluation of various platforms, including Ethereum, Quorum, Corda, and Hyperledger Fabric, underscores the need for a detailed comparative analysis. Kakarlapudi's systematic review of blockchain for consent management in healthcare, IoT, and data storage emphasises the technology's potential in these areas, despite challenges and limitations. Peng et al. (2021) further discuss the privacy risks and preservation technologies in permissionless blockchain, suggesting the need for a unified standard classification. Adlam and Haskins (2019) specifically apply permissioned blockchain to the authorisation process in electronic health records, demonstrating its potential to enhance data security. These studies collectively underscore the importance of blockchain technology in permission management, particularly in ensuring data privacy and security.

A prior study indicates that activity logs, especially in cases of fraud, illegal activities, or security breaches, are essential to audits (King, 2013). Audit logs can be altered or removed with ease. For critical or high-value systems, tamper-proof blockchain technology can be used to protect auditable activity records (Ahmad, Saad, Bassiouni and Mohaisen, 2018). Digital identities encompass historical data that forms the digital profile in addition to authentication details. These could include past purchases, browsing history, social connections, and personal or medical preferences. These datasets can be analysed by machine learning algorithms to create a precise and comprehensive picture of the user profile, which may or may not be to their advantage. Blockchain technology offers the potential to give individuals control over their personal data, enabling them to authorise its use only when they choose. This could represent a significant step toward enhancing personal privacy (Aydar *et al.*, 2019).

All the previously mentioned studies address the issue of authentication and privacy. Furthermore, we need to discuss studies that have been done in developing a security framework for data security in digital platforms. In their recent journal articles, Katkova, Tregubov, Kapustina, Yussuf and Pilipchuk (2020), and Elisa, Yang, Chao and Cao (2020) propose a blockchain-based secure and privacy-preserving e-government framework system. They show how blockchain technology can assist in secure records kept in a digital platform using public-key cryptography, which protects against malicious attempts at change and/or unauthorised access, while users are given private keys for validating and signing transactions. Digital signatures and encryption

are used by the network to guarantee document security, privacy, and access control. Additionally, because an attacker would need to control at least 51% of the network peers, most blockchain consensus algorithms make it nearly hard for them to alter data. More specifically, an attacker would have to change every copy of a block in the network before persuading most nodes that the modified block is legitimate in order to change any block in the blockchain (Elisa *et al.*, 2020).

Additionally, all user blocks are hashed, and an incomprehensible hash of the transactions is kept in the blockchain to increase the privacy of the data stored in the proposed network. The work of Katkova, Tregubov, Kapustina, Yussuf and Pilipchuk (2020), and Elisa *et al.* (2020) is limited to a theoretical framework and discussion. The framework's development and implementation are still in the works. Piscini and Kehoe (2018) determined that blockchain technology, with its inherent features of immutability, transparency, auditability, data encryption, and operational resilience, has the potential to enhance cyber defence. By securing data, preventing fraudulent activities through consensus mechanisms, and detecting tampering (while avoiding a single point of failure), blockchains could significantly improve cybersecurity (Piscini and Kehoe, 2018).

Another study (Ahmed *et al.*, 2019) created a model to provide smart parking solutions, a service-based platform based on infrastructure integration mechanisms using blockchain technology. This model is mainly concerned with enhancing security and privacy. According to their findings, blockchain technology has already significantly impacted decentralisation through cryptography. Their proposed model avoids transmitting personal or business strategy information via a trusted third party. Overall, the workflow they presented ensures a secure network for a service-based digital platform. Their research is also limited to the theoretical aspect.

The authors of Taylor *et al.* (2020) discussed about current studies that show how blockchain technologies can be beneficial in addressing cyber security problems. Several key research on the service-based digital platform choose to use smart contracts and the Ethereum platform to address their security concerns. Future studies might examine the different ways in which Ethereum and other permissioned or permissionless blockchain systems have been or might be used to develop cutting-edge cybersecurity solutions.

In a study by Cachin, Schubert and Vukolić (2017), Hyperledger blockchain fabric was proposed – a distributed open-source framework with pluggable functionalities due to its modular structure. It advances blockchain technology by providing an open-source platform for maintaining distributed ledgers. This Linux-based platform has the potential to transform the way businesses operate completely. Hyperledger is used by many blockchain-based products on the market.

To the best of the researcher's expertise, there appear to be very few systematic literature reviews on the application of blockchain in developing data security frameworks. One of the most recent survey studies on blockchain and cybersecurity was released in (2022) by Wylde et al. A thorough overview of the current blockchain-enabled techniques for authentication, confidentiality, privacy, access control, data and resource provenance, and integrity for such security service applications is provided by Wylde et al. (2022), who also focus on the challenges and issues associated with the use of centrally architected security services in various fields of application. From the perspective of the researcher, this effort is a good place to start when it comes to creating a blockchain-based framework that would protect data on service-based digital platforms.

However, although, previous studies have contributed to illuminating our understanding of the broader use of blockchain technology for data security, none of the previously mentioned studies have examined the use of blockchain technology and developed data security frameworks in service-based digital platforms, especially in the context of missionaries. Hence, there is a need for the current study to fill the gap in the literature.

In this research, we therefore develop a decentralised application based on blockchain technology to address these problems. It has a peer-to-peer architecture, which means that instead of storing data in a centralised server, data is stored at each node in the network and is encrypted. However, implementing blockchain technology will be difficult and will necessitate answering the following research questions:

- How has blockchain technology transformed the technology industry?
- To what extent is blockchain technology effective for developing a data security framework?

2.6. Summary

The findings of a literature review were presented in this chapter to establish the study's research focus. The chapter began by examining missionaries, their activities, and the logistical challenges they encounter. This section highlighted the need for secure, accessible, and affordable digital platforms tailored to the unique requirements of missionary organisations, forming the basis for the proposed blockchain-based framework. The review then transitioned to digital platforms, exploring their functionalities and inherent data security concerns. By identifying the limitations of existing platforms, particularly in service-based digital platforms, this section provided the rationale for adopting blockchain technology to address these challenges and enhance data security.

A detailed examination of data security frameworks followed, focusing on existing approaches and their components. This section emphasised the importance of confidentiality, integrity, and availability (CIA) in designing secure systems, establishing these principles as a cornerstone of the proposed framework. The chapter also investigated blockchain technology, its architecture, and its applications in data security. By demonstrating blockchain's capabilities, such as decentralisation, immutability, and transparency; the section justified its selection as the core technology for addressing the identified security gaps in service-based platforms.

Finally, the related work section reviewed prior studies on blockchain and data security, identifying gaps in existing research, particularly the lack of frameworks tailored to non-profit and service-based platforms. This analysis reinforced the study's objectives and highlighted the novelty of the proposed framework, which aims to address these gaps.

The next chapter will provide a detailed explanation of the study methodology, which includes the research paradigm, methodologies used, and the case study including participants, data collection methods, and analytical processes.

3. CHAPTER 3: Research Methodology

3.0. Introduction

The current chapter thoroughly describes the paradigm and research methodology used to achieve the study aim mentioned above. It also further discusses the research setting, sampling techniques, data collection techniques, validity, and reliability as well as data analysis, employed in this study.

3.1. Research Paradigm

A paradigm is a set of beliefs about how particular problems exist and a set of agreements on how such problems can be investigated (Fraser and Chris Robinson, 2004; Soraya, Binti and Kamal, 2019). There are four major research paradigms: positivism, interpretivism, post-positivism, and pragmatism (Mittwede, 2012; Wooi Keong and Md Husin, 2021).

Given the objective of this study (to investigate the feasibility of using blockchain technology in developing a framework for securing data for service-based digital platforms) and the main research questions (What are the benefits of implementing a digital platform for Global Mission Services? How has blockchain technology transformed the technology industry? To what extent is blockchain technology effective for developing a data security framework?), the pragmatist paradigm was selected as the most appropriate research paradigm for this study. The following are the reasons for this choice:

- This study intends to identify problems concerning digital platform data security. Thus, it is necessary to examine this from different perspectives (e.g., users' perception of online security, and the type of services exchanged online).
- This study addresses a complex real-world problem, namely evaluating the application of blockchain technology for data security by developing a blockchain technology framework for data security and a prototype of a digital platform for Global Mission Services (GMS), a topic about which very little is known.

3.2. Research Methodology

The term "research methodology" describes the systematic procedure that researchers employ to address the research question, collect data using a variety of techniques, analyse the findings, and reach conclusions (Ali Khan, Raman, Sambamoorthy and Prashanth, 2023; Vitale, 2023). As was mentioned earlier, mixed methodology and DSRM were applied in this study. The key characteristics of these two mentioned research methodologies are explained below.

3.2.1. Mixed-methods design

Mixed-methods design combines quantitative and qualitative methodologies in a single study to acquire a complete understanding of a research problem or phenomenon (Clark and Ivankova, 2016; Creswell and Creswell, 2017). To effectively address the objectives outlined in this study, a mixed-methods design integrating quantitative and qualitative methodologies was used. This choice is influenced by the realisation that quantitative data broadens and generalises the findings, whereas qualitative data adds depth and context, increasing the understanding of the subject under examination (Dawadi, Shrestha and Giri, 2021; Jackson-Gordon and Plano Clark, 2023). By combining the two methodologies (quantitative and qualitative), researchers can triangulate their findings, increasing study credibility and validity (Sharma, Bidari, Bidari, Neupane and Sapkota, 2023). Hence, in the context of this study, the mixed-methods design was used to provide a full understanding of the research problem, utilising the strengths of both quantitative and qualitative methodologies to deliver robust insights and support informed decision-making.

Quantitative Methodology

Quantitative methodology was utilised to explore and analyse the intricacies of missionary travels and operations. This quantitative aspect provided valuable insights into the nuanced aspects of service-based digital platforms for missionaries and aided in identifying the operations and the kind of services that need to be secured. These insights were instrumental in identifying the types of services and operations that need to be secured within service-based digital platforms.

Qualitative Methodology

Qualitative methodology was employed to assess the effectiveness of the developed framework and prototype, particularly in terms of its impact on enhancing data security. This involved evaluating the prototype by creating and testing a distributed application running on the Ethereum network. The testing process was designed to validate the framework's adherence to the CIA Triad principles of Confidentiality, Integrity, and Availability.

By combining both quantitative and qualitative methodologies, this study aims to ensure a comprehensive and robust examination of the feasibility and efficacy of utilising blockchain technology in securing data for service-based digital platforms, specifically developed for missionary institutions in South Africa and Eswatini.

This design was selected for two reasons. The initial phase conducts quantitative data collection and analysis. The second phase conducts qualitative data collection and analysis. In the context of this study, a quantitative methodology was used in the first phase to help select participants, while the second phase, which was qualitative methodology, investigated how participants felt about the security of their online data. The combination of qualitative and quantitative methodologies (mixed methods) made it easier to fully understand the requirements of missionaries in South Africa and Eswatini, which helped to develop a digital platform that met their needs.

3.2.2. Design Science Research Methodology

Design Science Research Methodology (DSRM) is a problem-solving paradigm that aims to improve human knowledge by creating novel artefacts (vom Brocke, Hevner and Maedche, 2020; Hevner and Park, 2004). Researchers use the DSRM to solve problems using innovative ideas through evaluating and developing artefacts. The artefact development employs the processes for Design Science in Information Systems. Several DSRM processes in information systems have been developed (Chatterjee, Sundarraj and Dutta, 2023). Some examples of these processes include the DSRM proposed by Hevner and Park (2004), the six-step process model proposed by Peffers, Tuunanen, Rothenberger and Chatterjee (2007), the Design Science Research Process Model (DSR Cycle) by Vaishnavi and Kuechler (2004), and so forth.

However, the existing literature shows that Hevner and Park's DSRM is the most preferred due to the completeness of the processes involved in the development of artefacts, particularly in the context of information systems (Haryanti, Rakhmawati, Subriadi and Tjahyanto, 2022). Hence, the DSRM proposed by Hevner and Park was adopted in this study. Hevner and Park's process consists of six stages, which are explained in detail regarding their implementation in this study in Table 3.1 below.

Table 3.1. Design science process (Hevner & Park, 2004)

	Process	Description
1.	Problem identification and motivation	Many valuable services offered by missionaries remain invisible to people who need them because they lack easily accessible information about these services. Integrating these services into one platform is the solution to this. However, information in digital platforms stored in the cloud may breach the privacy of sensitive information.
2.	Objectives of a solution	This study's main objective is to investigate the viability of using blockchain technology to develop a framework for securing data for service-based digital platforms.
3.	Design and Development	Artefact: Design a blockchain framework to secure data for service-based digital platforms.
4.	Demonstration	Developing the GMS digital platform prototype to address the security issues of digital platforms.
5.	Evaluation	Evaluate the GMS platform. Applying the developed framework theory in an experimental digital platform prototype simulation to determine if it meets all the requirements.
6.	Communication	Communicates the problem and its significance, the framework, the thoroughness of its development, and its effectiveness to researchers and other relevant audiences as needed.

The study employed Hevner and Park's (2004) six-phase Design Science Research (DSR) methodology as shown in Table 3.1 above, to create two artefacts namely the GMS digital platform and the Blockchain Technology for Data Security framework.

This combination of DSRM and the mixed-method design improved the reliability and relevance of the developed solutions by aligning them with cybersecurity standards while also meeting the research of the study.

3.3. Case Study of Missionaries in Eswatini and South Africa

3.3.1. Research setting

There are many missionary centres around the globe that provide assistance in various areas of human need, such as accommodation, healthcare, and education (Alawode, 2016; Loewenberg, 2009). This study focused only on missionary centres located in Eswatini and South Africa. Eswatini and South Africa were selected as the study locations because of their practical accessibility, which facilitated the data collection and direct communication with missionaries. Furthermore, selecting these locations also facilitated cost-cutting on international calls and travel expenses.

3.3.2. Sampling techniques

For this study, purposive sampling was applied to select participants of the study which helped in aligning the research with the study's objectives and purpose. The decision to use purposive sampling was based on the following considerations:

- The study focused on examining the effectiveness of using blockchain to secure information in digital platforms, aimed specifically at missionaries in South Africa and Eswatini, in order to be able to share information and activities safely online. This suggests that missionaries were the digital platform's intended users.
- The target users of the digital platform were missionaries operating online. As a result, it was critical to learn about their attitudes about online security.
- The researcher possessed prior knowledge of where to locate these missionary centres.

This approach facilitated the selection of missionary centres that could provide valuable insights into the digital platform functionality to make sure it meets the missionaries' requirements.

3.3.3. Participants

The participants for this study were selected from the Southern African Catholic Bishops' Conference Directory, which provided a thorough list of contact information for missionary centres. Participants who were approached at random and asked to participate in the study were given a brief explanation of the study's goals. The initial approach entailed contacting these centres by phone to explore their interest in participating in the study. Missionaries were chosen as the target group; firstly, because within their network, the researcher observed a critical need for the development of a digital platform to enhance information sharing. Secondly, missionaries play essential roles in society, therefore their viewpoints are useful for assessing the potential influence of such a platform. For the remainder of this chapter, the term participants will be used when referring to missionaries.

3.3.3.1. Ethical clearance procedures and ethical considerations

Before starting to collect data, the designed questionnaire was first submitted to the Central University of Technology, Free State, Faculty of Engineering, Built Environment, and Information Technology (FEBIT) Postgraduate Research Committee for review and approval. After approving the questionnaire, the committee issued an ethical clearance to the researcher (see Appendix 4).

To ensure that the research followed ethical guidelines, all the participants received an explanation of the background of the study and its implications, assuring them that their participation was voluntary and providing them with consent and confidentiality forms (see Appendix 3). During surveys, anonymity was also maintained; for privacy reasons, the participants were not identified. Participants also received a copy of the ethical clearance approval document to confirm that the research was conducted solely for research purposes.

3.3.4. Data collection techniques

As explained below, data collection was done using survey and system testing to ensure the data accuracy.

3.3.4.1. Survey

The surveys, in the form of questionnaires, were designed with questions ranging from basic technical information to subject-specific details. The objective was to collect information about the GMS digital platform prototype and framework's development. The responses to the questionnaire assisted in determining whether the development of this platform would meet the needs of missionaries in Eswatini and South Africa.

This study used closed-ended questionnaires to learn about missionaries' opinions or beliefs on the feasibility of the GMS digital platform. The closed-ended questionnaires consisted of two types namely the selection questionnaire and the online security and website usage questionnaire to guarantee that the data collection was in line with the research objectives.

Selection Questionnaire

The selection questionnaire (see Appendix 1) aimed to gather comprehensive information regarding the missionary centres that are currently in operation in Eswatini and South Africa. It was divided into four separate sections to guarantee clarity and effectiveness in the collection of data.

The first section focused on organisational information and geographical location. The second section contained questions related to the organisational operational details. In the third section, participants were requested to elaborate on the services offered by their centres. This included specifying the types of services provided and explaining the primary purposes for guests' visits. Finally, the fourth section's questions concentrated on information technology. Section four's primary objective consisted of determining which centres had a website. This information was critical as it determined eligibility for participation in the next phase of the study.

Online Security and Website Usage Questionnaire

The online security and website usage questionnaire (see Appendix 2) was aimed at finding out about participants' perceptions of online safety and website usage through a structured questionnaire divided into two sections.

The first section discussed the website's aim as well as how to use electrical equipment. Participants were asked to describe the principal objective of their website and the electronic devices they used when browsing it. The second section focused on participants' perceptions of online security, following a linear method linked with the three CIA principles of Confidentiality, Integrity, and Availability. Participants evaluated aspects of confidentiality, including authentication, authorisation, and accountability. Integrity questions focused on the potential compromise of information, whereas availability questions investigated participants' experiences with website downtime and access denial.

3.3.4.2. System testing

The purpose of using online testing was to thoroughly evaluate the digital platform prototype's safety, reliability, and effectiveness. The researcher aimed to ensure the platform's resilience across key aspects including Confidentiality, Integrity, and Availability through running the platform through a variety of testing scenarios.

MetaMask was used to evaluate the prototype to ensure strong authentication, authorisation, and availability which formed the framework's confidentiality component. It was also used to evaluate the integrity of the prototype. Hardhat was used on the local development network to test and evaluate smart contracts to ensure integrity. Smart contracts were then deployed to an online network called Polygon Infura which is an Ethereum network to see if they complied with all data integrity criteria. Finally, it was uploaded to a distributed database called IPFS to evaluate the system's availability.

3.3.5. Validity and reliability

To evaluate the quality of the data collection, validity and reliability checks were performed as follows:

3.3.5.1. Validity

The term validity refers to how accurately a measurement instrument measures what it is designed to measure (Cohen, Manion and Morrison, 2017; McKim, 2022). It includes both the efficacy and accuracy of the measuring instruments. This study used internal and external validity. Internal validity ensures reliable measurement, whereas external validity refers to the generalisability of findings beyond the study group. Johnson and Christensen (2014) advocate for gathering several sources of validity evidence, while Dawadi et al. (2021) emphasise the advantages of mixed methods over single-method approaches for avoiding biases and increasing validity.

This study used a mixed-methods design for a thorough investigation and increased validity. A representative sample of missionary centres in Eswatini and South Africa was used, and all examinations and questions were specific to the research objectives. Data analysis was conducted using content analysis approaches to uncover trends and concerns.

3.3.5.2. Reliability

Reliability is known as the capacity of a research finding to show that comparable outcomes would be attained if the study were repeated with a similar sample of respondents in a similar setting (Cohen *et al.*, 2017). In simple terms, reliability refers to the constancy of a measure. According to Lazar, Feng and Hochheiser (2017), Reliability checks encompass two dimensions: reproducibility and stability. Reproducibility is the consistency of the measured items across several tests, whereas stability is the consistency over time and with similar samples. As a result, Johnson, Adkins and Chauvin (2020) suggest that researchers publish extensive explanations of their methodology in order to justify their conclusions.

Other researchers may be interested in duplicating this study. Recognising that conditions may change during replication, this study sought to provide a complete overview of the decisions and processes used. To maximise the chances of successful

replication, all goals, objectives, and justifications for the research paradigm and methodologies, as well as specific decisions and procedures, were explicitly defined.

3.3.6.Data analysis

Quantitative data analysis, including participants' organisational information and activities, along with qualitative data analysis focusing on participants' perceptions of online security, were derived from the survey used for data collection. The analysis of both types of data was conducted using R Studio, ensuring a robust and systematic approach to interpreting the results.

Quantitative analysis was used to:

- Compare data on participants (missionary centres) to identify the needs and crucial perspectives of missionaries working in the diverse landscapes of South Africa and Eswatini.
- Collect data to ensure that missionary centres adhered to the profile of the target potential study participants.
- Provide data in the form of compiled and statistical data.

In addition, this study included qualitative analysis in order to:

- Learn more about the purpose of the missionaries' websites, their electronic equipment usage patterns, and their perceptions of online security.
- Provide data in the form of compiled and statistical data.

The combination of the two data types indicated above enabled a more comprehensive understanding needed to assist decision-making, as well as the production of new data, which might enhance the study's quality. Conclusions were drawn using the results of the researcher's comparative statistical test analyses of the survey. These conclusions assisted the researcher in understanding the missionaries' requirements in terms of the geographical location, services offered by missionary centres and guest visit purpose, online presence information (website information), purpose of website and electronic usage and participants' perceptions of online security.

The researcher was then able to:

- Identify different geographical location needs of missionaries and provide detailed information on the services offered by missionary centres based on various purposes of guest visits which helped in the development of the GMS digital platform.
- Incorporate participants' perceptions of online security to ensure trust and safety.

The detailed clarification of the data analysis is displayed graphically (see Appendix 5).

3.4. Summary

This chapter described the methods used to carry out the study. To achieve the main research objective, the study used a mixed methodology combining quantitative and qualitative data. In addition to the mixed methodology, the Research Design Science Methodology was also used. Data were collected through surveys, literature review and online testing of the digital platform. The data were analysed, and issues of validity and reliability were discussed. Ethical concerns and clearance procedures were also considered and described. In the following chapter, the development procedure of the blockchain framework will be covered in detail.

4. CHAPTER 4: Framework Development Process

This chapter outlines the development of the blockchain framework for data security in digital platforms.

4.0. Introduction

This chapter presents a detailed framework for securing data in service-based digital platforms and outlines its development process. This chapter also identifies and explains the framework's components based on the literature review, followed by the Design Science Research Methodology (DSRM). The framework development is demonstrated.

4.1. The Framework's Rationale

Data security is becoming increasingly important in the rapidly developing digital era as businesses deal with an increasing number of cyber threats aimed at their sensitive data. Although there is some effectiveness to the data security procedures that are now in place, there are still certain restrictions and flaws, as highlighted earlier, these limitations pose tremendous obstacles to maintaining complete data protection in accordance with the CIA Triad model's principles of **Confidentiality, Integrity, and Availability**.

Through the development of the proposed blockchain framework, this research seeks to address the weaknesses of traditional data security methodologies and create a more robust solution based on the CIA Triad model based on blockchain technology. The suggested architecture aims to strengthen data confidentiality, integrity, and availability by strategically integrating decentralisation, immutability, consensus mechanisms, smart contracts, and transparency, thereby reducing possible threats and enhancing overall data security. The process of creating the blockchain framework adheres to a systematic methodology, drawing on the principles of Design Science Research, opening the door for its practical implementation and possible adoption in real-world applications.

4.2. Blockchain Framework Building Process

A comprehensive literature review on the application of blockchain technology for data security in service-based digital platforms informed the creation of the proposed framework. This framework offers a practical and comprehensive approach to safeguarding platform data and provides best practices for developing secure software applications. It serves as a guide for software developers and stakeholders in creating and managing secure digital platforms. To address the gap in existing frameworks, this study integrates insights from both the literature and empirical data to propose a blockchain-based solution tailored specifically to the unique security challenges faced by service-based digital platforms. The blockchain framework was developed using Peffers' (2006) Design Science Research (DSR) methodology, as illustrated in Figure 4.1.

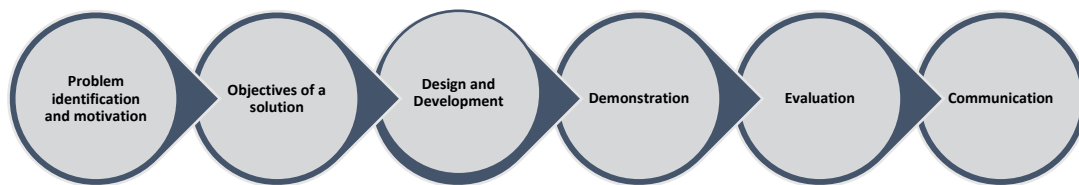


Figure 4.1. The Design Science Research

4.2.1. Phase 1: Identification of the problem

From the literature review that was conducted, the issues that the proposed blockchain architecture aims to solve were identified. From this, the framework aims to address the weaknesses in current data security methods as well as the risks created by centralised data storage. Furthermore, the framework intends to provide a more secure and transparent way to securing sensitive information by leveraging the decentralised and immutable properties of blockchain technology, considerably advancing data security in the digital age.

4.2.2. Phase 2: Definition of objectives for a solution

The objective for the proposed blockchain framework was identified as the improvement of data security in service-based digital platforms by using the benefits of blockchain technology. A decentralised design was also identified as means of

reducing the possibility of single points of failure, strengthening resilience against future cyber-attacks. In addition, the immutability of data transactions ensures the accuracy and dependability of information, while the openness it provides encourages user trust. Notably, the framework follows the theories of Design Science Research, displaying a methodical approach that makes practical implementation and future adoption in real-world applications easier. As a result, it aids greatly in creating a safer and more secure data environment.

4.2.3. Phase 3: Design and development of the blockchain framework for data security

This phase comprises six steps, namely: Component identification, relationship simulation, architecture of the developed framework, and framework composition.

4.2.3.1. Component identification

The framework was designed following the CIA Triad framework, employing blockchain for every component. After reviewing the work of previous scholars, the CIA Triad was utilised to create the framework which consists of confidentiality, integrity and availability.

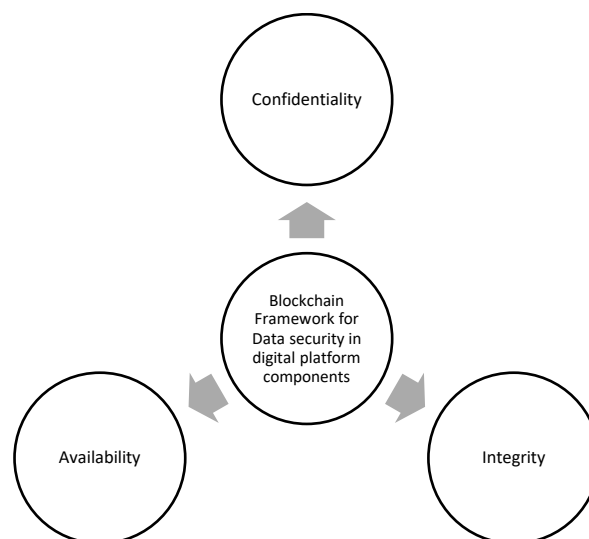


Figure 4.2. Blockchain framework for data security in digital platform components

4.2.3.2. Relationship between components

R1: Confidentiality – Integrity

When it comes to data security in digital platforms, confidentiality and integrity are closely related components. Confidentiality refers to the safeguarding of sensitive and personal information from unauthorised access or exposure (Keung, 2013). Integrity, on the other hand, is concerned with maintaining the accuracy and consistency of data (McBride, Townsend, Ekstrom, Lusty and Sexton, 2018). The relationship here underlines the importance of protecting confidential information to ensure the data's reliability and credibility. By keeping data confidential, unauthorised modifications or tampering can be avoided, preserving data integrity (Muthurajkumar, 2021).

R2: Confidentiality – Availability

The relationship between confidentiality and availability emphasises how crucial confidentiality protections are to guarantee a system's availability. When sensitive data is not properly maintained, there is a possibility of security lapses or illegal access, which may cause system inaccessibility (Valecha, Rudek, Szczepanik and Palus, 2021). Confidentiality allows the system to better defend itself against potential assaults and security errors, enabling its availability and ongoing operation (Khan and Babay, 2021).

R3: Integrity – Confidentiality

The relationship between integrity and confidentiality emphasises the point that sustaining data confidentiality depends on maintaining data integrity. Sensitive information may be accessed or disclosed without authorisation if the integrity of the data is compromised (Prasuna, Sermakani and Paruvathavarthini, 2020), for example, if it has been unlawfully altered or tampered with. The system guarantees that private information is kept secure and preserved from unauthorised parties by maintaining data integrity (Chaitanya *et al.*, 2021).

R4: Integrity – Availability

Integrity and availability are related because maintaining system availability requires data integrity. Data consistency and reliability assure the accuracy and dependability of the stored information and promote the system's efficient operation (Chicco, 2021).

Data integrity makes it possible for the system to run more efficiently, which ultimately increases the system availability (Shashi, Yadav and Mishra, 2020).

R5: Availability – Confidentiality

The relationship between availability and confidentiality emphasises the importance of assuring a system's availability in order to maintain confidentiality. If a system experiences frequent outages or disturbances, it may be more vulnerable to security breaches or illegal access, potentially leading to data leaks (Bommannavar and Bambos, 2011). By ensuring system availability, the risk of illegal access is reduced, improving data confidentiality (Feng and Zhang, 2017).

R6: Availability – Integrity

The relationship between availability and integrity highlights the importance of system availability in preserving data integrity. A system that endures frequent downtime or interruptions may result in data corruption, loss, or other integrity-related issues (Alhussen and Arslan, 2021). Data integrity is improved by assuring the system's continuous operation and quick response to user demands, resulting in more reliable and accurate information within the system (Alyami and Almutairi, 2021).

4.2.3.3. Framework architecture design

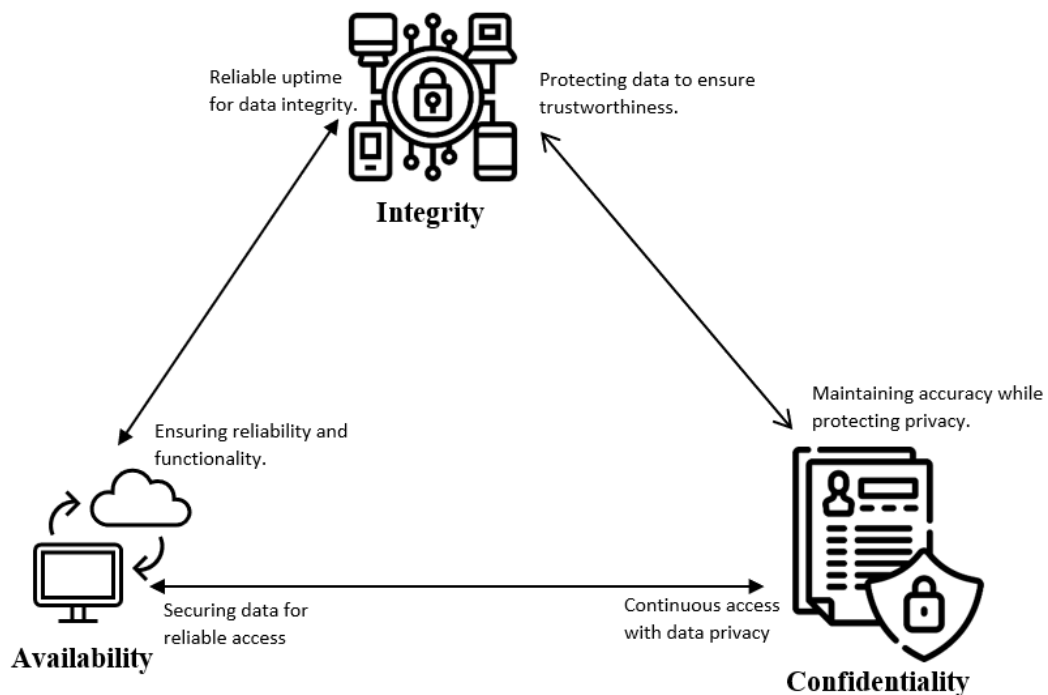


Figure 4.3. Framework architecture design

The framework architecture design shown in Figure 4.3 forms the foundation of a secured service-based digital platform. Confidentiality, integrity, and availability – three essential components are depicted in this graphic effectively highlighting their crucial links. Each element guarantees the system's efficacy, serving as the framework's pillars. The first connection between confidentiality and integrity emphasises protecting private data to maintain its reliability and accuracy. Figure 4.3 demonstrates how these two aspects are intricately connected, emphasising the importance of maintaining confidential data to ensure total data reliability.

Furthermore, the second relationship emphasises the critical relevance of data security in ensuring continuous and dependable system access. By adding rigorous confidentiality safeguards, the system can prevent unwanted access and breaches, increasing its overall availability. The third connection underlines the importance of data consistency and reliability in providing seamless system access for users. Data integrity ensures the system maintains confidentiality and availability, thereby improving the user experience. Developing a service-based digital platform that follows this framework architecture design will guarantee a secured system that covers the essential components of confidentiality, integrity, and availability, making a well-secured system. In the next section, blockchain technology mechanisms are added to this framework to apply its mechanism to guarantee that each component meets all the requirements.

4.2.3.4. Blockchain technology framework using the CIA Triad model

The proposed blockchain framework, depicted in Figure 4.4, is an architecture that improves the fundamental concepts of the CIA Triad. These layers (Confidentiality, Integrity, and Availability) have been precisely built to strengthen data security through blockchain technology mechanisms. This framework incorporates Ethereum's principles, such as decentralisation, smart contract functionality, and immutability, to enhance data security mechanisms. The design is informed by existing literature and represents an evolution of the Ethereum framework adapted to this study's specific objectives.

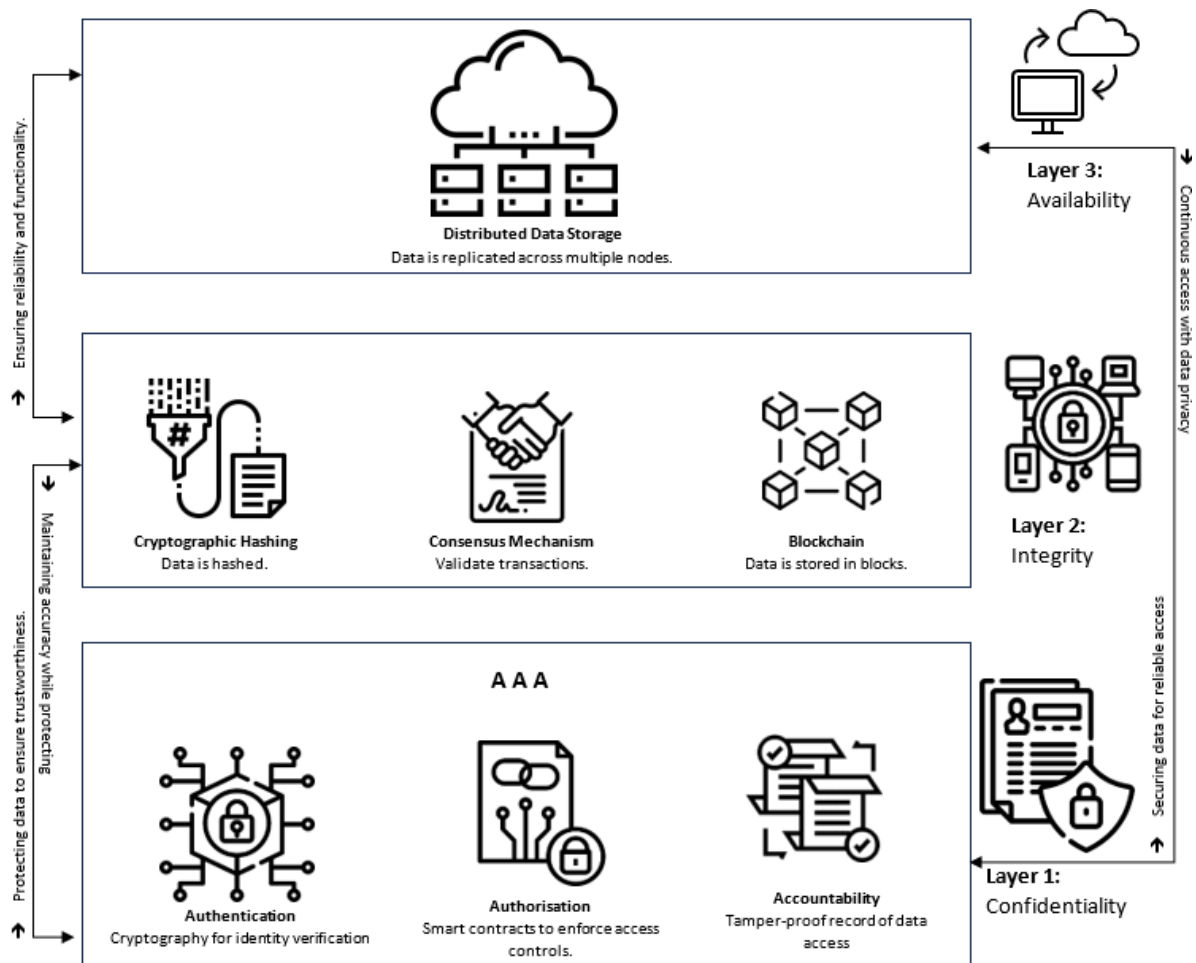


Figure 4.4. Blockchain technology framework using CIA Triad model architecture

Confidentiality is at the forefront, a pillar of user confidence strengthened by cryptographic techniques. Cryptography is used in authentication to establish identities. In addition, Authorisation makes use of smart contracts to guarantee regulated access. An unchangeable data access record is a virtual audit trail to promote accountability. As we move on to **Integrity**, we come across three processes that protect the fundamental components of data. Cryptographic hashing prevents any illegal changes. While this happens, consensus processes validate and permanently store transactions inside immutable blocks. **Availability** is achieved using a distributed data storage architecture. This method spreads data over several nodes, reducing the danger of data loss from a single point of failure. This redundancy ensures constant access to crucial information despite hardware malfunctions and hostile breaches. Due to this, operational resilience is ensured even under challenging circumstances.

4.2.4. Phase 4: Demonstration

The Global Mission Digital (GMS) Platform prototype was successfully created as part of this phase. The next chapter provides a detailed explanation of the prototype's design. This part provides an immersive and dynamic development process, clarifying the platform's numerous functionalities. The GMS Digital Platform is a novel digital platform built on the foundation of blockchain technology. Adopting the Ethereum blockchain as its underlying structure, this platform uses the security and transparency built into the network, enabling impenetrable and decentralised transactions. The prototype is a demonstrative example, highlighting how blockchain technology may strengthen data security in service-based digital platforms.

4.2.5. Phase 5: Evaluation

The evaluation process, which thoroughly tests each layer of the framework to ensure it complies with blockchain requirements, is highlighted in the next chapter. The framework's adherence to blockchain principles, such as data immutability and consensus, as well as its security procedures, prioritising confidentiality, integrity, and availability, are validated during this dual-purpose phase. The evaluation phase combines practical application with theoretical blockchain ideas. It improves the fidelity and toughness of the prototype, making it more capable of navigating the complex blockchain environment.

4.2.6. Phase 6: Communication

The effective communication of the research findings and the blockchain framework to relevant stakeholders, especially the missionaries in Eswatini and South Africa, was methodically planned to maximise impact and outreach. The targeted communication approach aimed to ensure the dissemination, comprehension, and potential adoption of the research outcomes in real-world applications.

- 1) Research Publications:** Two peer-reviewed research papers were published in two conferences, IST Africa and a book chapter at the EAI AFRICATEK Conference to disseminate this study's results to the academic community and beyond. These publications provided a thorough description of the evolution of the blockchain architecture for data security, serving as a reliable source of

knowledge. By choosing a respected conference, it was ensured that the research was widely known among academics and industry experts.

- 2) **Online Resources:** The power of online resources was employed by hosting the blockchain platform on a live network accessible to all stakeholders. The stakeholders were provided with a link to access the platform, which was accompanied by a comprehensive user manual to guide them effectively. This online resource allowed stakeholders to engage with the platform firsthand and explore its potential applications. The platform source code is available on GitHub, and the actual platform is hosted on a distributed Fleek network.
- 3) **Training Sessions:** Upon the project's completion, the researcher plans to organise a training session specifically for the missionaries. This training session will provide them with essential knowledge and skills on how to use the GMS digital platform effectively. The aim is to empower the missionaries to fully leverage the platform's capabilities and understand its potential impact on their operations.

4.3. Conclusion

The chapter presented the framework design process. It outlined the rationale behind designing a framework to ensure excellent digital platform development, guaranteeing data security. The rise of cyber-attacks motivated the development of this framework based on findings presented in section 2. The model development process involved a literature review, engaging missionaries from South Africa and Eswatini through data collection and identifying their activities and online data security experience. The main components of the proposed framework, confidentiality, integrity, and availability were described.

5. CHAPTER 5: Framework Implementation

5.0. Introduction

This chapter details the practical application of the blockchain framework designed for data security, as outlined in the previous chapter. The current chapter is structured into two sections: the demonstration and the evaluation. The demonstration phase involved the development of the Global Mission Services (GMS) digital platform. This development was informed by a survey distributed to missionaries in Eswatini and South Africa, aiming to better understand their needs and preferences to design a platform customised to their requirements. The survey comprised two phases: a selection questionnaire followed by an evaluation of the missionaries' perceptions of online security. The survey results are thoroughly examined in this chapter, along with how they affected the development of the GMS digital platform. It also explores how the blockchain framework might be used in practice to meet the missionaries' needs, which is consistent with the technology covered in Chapter 2 and the framework introduced in Chapter 4. This in-depth investigation seeks to confirm whether the developed blockchain framework can satisfy the unique requirements of missionaries in South Africa and Eswatini.

5.1. Framework Demonstration

The researcher emphasises the practical use of the blockchain framework in this phase by developing a prototype for the GMS digital platform. As an example, the GMS platform works to increase user confidence and transparency across the network of Eswatini and South African missionaries. The primary goal of this part is to clarify the efficacy and value of the evolving blockchain framework in efficiently tackling the complex difficulties associated with data security. The researcher elaborates on the GMS prototype's development process, providing a complete overview.

5.1.1. Specification requirements of the GMS

Before the requirements of the digital platform were outlined, a thorough survey was carried out to identify the needs and crucial perspectives of missionaries working in the diverse landscapes of South Africa and Eswatini. This survey formed the basis for determining which GMS platform components were necessary. The survey was done in two phases. The first phase consisted of the selection questionnaire which served

the purpose of screening all missionaries operating in South Africa and Eswatini to ensure that they adhered to the profile of the target potential study participants. Hence, the questions contained in the selection questionnaire sought to collect the following information about existing missionary centres in South Africa and Eswatini: their regional location, the kinds of services they provided, the purpose of visit for most of their guests, and their online presence. The second phase of the survey concentrated only on missionary centres that adhered to the profile of the target of the study participants. This selected group of missionary centres were further requested to complete the second phase of the survey. The second phase survey's questions focused on learning more about the purpose of the missionaries' websites, their electronic equipment usage patterns and their perceptions of online security. The following subsection presents the survey data analysis results related to the two survey phases, respectively, including important conclusions made from the survey, which informed the development of the platform.

5.1.1.1. Survey results and findings

- **Geographical location**

There was a total of 64 missionary centres that participated in the first phase of this study of which 95.31% were located in South Africa and 4.69% in Eswatini. This is an indication that nearly all these missionary centres were based in South Africa, with a smaller presence in Eswatini. Mostly, the questionnaires were answered by receptionists (28%), followed by administrators (20.4%), managers (14.1%) and HR (6.4%), with others contributing towards <1%. Note that for the remainder of this chapter, the term participants will be used when referring to missionary centres.

- **Services offered by missionary centres and guest visit purposes**

All participants (100%) offer workshop and retreat facilities. Furthermore, they confirmed the following are the purposes guests visit their centres: religious purposes (62.4%), leisure (18.8%) and business (18.8%). Based on the information, it can be noted that workshop and retreat facilities are the two kinds of services offered by all the participants. Also, guests mainly use these centres for religious purposes with others coming for leisure or business.

- **Website information**

Most participants (76.6%) had a website; the remaining 23.4% did not have a website. This is an indication that a majority of participants have an online presence.

As mentioned earlier, the second phase of the survey data collection focused only on participants who adhered to the profile of the target of the study participants. The results of the website information data analysis revealed that only 49 out of 64 participants (76.6%) fulfilled the characteristics of the target population in this study. Therefore, participants who did not fulfil the characteristics of the target population were excluded from the data analysis presented in the next two subsections, namely purpose of website and electronic equipment usage and participants' perceptions of online security.

- **Purpose of website and electronic equipment usage**

The majority (52%) of participants confirmed that they utilise their website for advertisement, 38% for both booking and advertisement, and 10% for online booking only. According to device usage, most participants use a computer to handle the website (56%), followed by tablets (16%), cell phones (16%) and other kinds of devices (12%). The data about the website's purpose revealed that there were differences among participants in terms of their website utilisation patterns. More than half use the website for advertisement, while others also use it for booking and advertisement, and only a small portion use it for online booking only. Additionally, computers are the most used devices to access these websites.

- **Participants' perceptions of online security**

Participants' perceptions of online data were collected using a Likert scale questionnaire. Participants could select one of the five Likert scale response options, namely strongly disagree, disagree, not sure, agree, and strongly agree to rate their perceptions of online security. The questions were organised into three categories: confidentiality (authentication, authorisation, and accountability), integrity, and availability. Table 5.1 shows descriptive statistics (mean and standard deviations (STD)) based on the scores for each statement, as well as the proportions of missionary centres that responded with strongly disagree (SD),

disagree (D), not sure (NS), agree (A), or strongly agree (SA). N is the number of respondents. The total of A and SA is shown. Again, the sum of A and SA was utilised to analyse and compare each participant's perception of online data security.

Table 5.1. Online security data

Category	Statement	N	SD	D	NS	A	SA	Sum of A and SA	Mean	STD
Confidentiality	Authentication I worry about the security of my password online.	49	1	13	14	21	0	21	3.08	0.92
			2%	26.5%	28.6%	42.9%	0%	42.9%		
	Authorisation I have experienced the loss of my sensitive personal information online because of a digital attack.	49	1	0	8	31	9	40	3.92	0.78
			2%	0%	16.4%	63.3%	18.3%	81.6%		
	Accountability I care about how the website and social media owners use my personal information.	49	0	2	14	26	7	33	3.74	0.78
			0%	4%	28.6%	53.1%	14.3%	67.4%		
Integrity	My personal information has once been compromised online.	49	1	12	11	25	0	25	3.2	0.90
			2%	24.5%	22.4%	51.1%	0%	51.1%		
Availability	I have been denied access to my website or my social media account.	49	2	18	16	13	0	13	2.82	0.87
			4.1%	36.7%	32.7%	26.5%	0%	26.5%		

a) **Confidentiality:** The confidentiality category was divided into three sub-categories: authentication, authorisation, and accountability. According to authentication data, a significant proportion (42.9%) of participants strongly

agreed/agreed that they worry about their password security online. The authorisation insights reflect that a substantial proportion of participants (81.6%) respectively strongly agreed/agreed that they have experienced the loss of sensitive information online because of unauthorised access. In terms of accountability, a considerable proportion of participants (67.4%) strongly agreed/agreed that they care about the information that they are accountable for, and how it is being used by the owner of the platforms they use. The result of the data analysis suggests that participants are concerned about the security of their passwords online, indicating authentication issues. The data also shows that a substantial proportion of participants have lost critical information as a result of forbidden access, raising concerns about the authorisation process. Furthermore, a considerable number of participants are concerned about how platform owners utilise user information, highlighting the growing desire for transparency and accountability on digital platforms.

- b) Integrity:** In the data integrity category, the majority of participants (51.1%) strongly agreed/agreed that their information had once been compromised online. This demonstrates a significant level of concern among participants regarding the integrity of their online information.
- c) Availability:** Regarding the availability of online services, a proportion of users (26.5%) strongly agreed/agreed that they have once been denied access to their website or social media platform. This implies that a fraction of respondents has experienced disruptions in accessing online services.

Taking into account the results of the two-phase survey presented and discussed above, it can be concluded (summarised) that the collected data reveals some notable trends within the surveyed participants. Firstly, there is a significant geographical concentration of missionary activity, with the majority of centres located in South Africa. Secondly, these centres provide a variety of services, offering workshops and retreats predominantly for religious purposes. Thirdly, the majority of centres have websites. Furthermore, the findings show that most participants use their websites primarily for advertising and booking, with a preference for computers over other devices. Lastly, with regard to participants who have a web presence, they expressed concerns about password security, authorisation, information usage by digital platform

owners, data integrity, and the availability of online services, emphasising the importance of addressing these issues to ensure a secure and reliable online experience for missionary operations.

5.1.1.2. Motivation for collecting data

The main purpose for collecting and analysing this data was to guide the development of the GMS digital platform. The goal was to efficiently design the digital platform to meet the requirements of missionaries by thoroughly exploring their geographical locations, the diversity of services they provide, their current online presence, and their perception of online data security.

The geographical location of missionary centres is critical in the development of an integrated digital platform because it helps with the optimisation of content and allows for focused outreach efforts, resulting in an efficient and impactful digital platform that is aligned with the missionaries' needs. Knowledge about the services offered by missionary centres and guest visit purposes provides important information about the types of data that must be protected within the platform. This ensures the platform's adaptability to accommodate the varied needs of missionaries engaging in different activities, enhancing its overall effectiveness, and addressing the complex requirements of the missionary community.

Website information provides critical insights into the centres' online presence to understand their online security perception. Importantly, the data on website usage provide critical information on how they use their website. Studying website usage is motivated by the goal of improving digital interfaces for missionary activities and communication. Concerning device preference, this is necessary to customise the digital platform for the best experience and to ensure alignment with missionaries' chosen devices.

On the other hand, examining missionaries' perceptions of online security is necessary to address their concerns, improve data protection protocols, and build trust in digital interactions. Concerns related to confidentiality, integrity, and availability, highlighted in the survey, guide the development of strong authentication protocols, secure transactional features, and reliable platform infrastructure. The GMS digital platform aims to provide a secure and user-friendly environment, ensuring the confidentiality of

sensitive data, maintaining the integrity of online transactions, and assuring continuous availability for the missionaries it serves.

5.1.1.3. Usage of collected data

Using the two phases' survey findings (results) in conjunction with the literature review described in Chapter 2, several critical characteristics of the platform were determined:

- 1) Easy access and transactional capabilities:** The platform should be designed to meet the specific requirements of missionaries, allowing them to publish and advertise their facilities based on their geographical location. The online platform should include a streamlined booking system to schedule workshops and retreat centres. Additionally, personalised user accounts should allow missionaries to handle bookings. The online platform therefore includes a streamlined booking system to schedule workshops and retreats. Additionally, personalised user accounts allow missionaries to handle bookings. The platform must have user-friendly access to information and transactional capabilities, such as an intuitive and desktop-friendly interface that ensures smooth navigation. It should have a responsive design which adapts to different devices, such as desktop computers, tablets, and mobile phones, based on user choices.
- 2) Confidentiality:** Strong security measures are required to protect confidentiality since it is essential to prevent unauthorised access to and exposure of sensitive data.
- 3) Data Integrity:** For the platform to gain users' trust, it is crucial to ensure the reliability and accuracy of data and transactions.
- 4) Availability:** By guaranteeing its continuous availability and seamless user experience, missionaries will have easy access to the services and information they need to complete their critical work efficiently.

Based on the survey findings, it is recommended to prioritise the development of the GMS digital platform as follows:

- 1) Integrity:** User concerns about ensuring data integrity should be addressed.

- 2) **Confidentiality:** Prioritise safeguarding passwords, protecting sensitive data, and preventing unwanted access and potential data loss.
- 3) **Availability:** The platform should be made more broadly accessible.

The GMS digital platform needs to efficiently meet the particular requirements of missionaries, improve user confidence, and encourage openness in their activities by adhering to this prioritised strategy.

5.1.2. Blockchain technology implementation of CIA Triad

The technology stack chosen for the prototype development of the GMS digital platform included several key components:

1. Easy access and transactional capabilities

As mentioned in the literature review, there are many tools and frameworks for digital platform development. Based on the substantial literature review conducted for the current study, **ReactJS** was the best fit for coordinating the platform's front-end architecture. ReactJS appears as a supremely efficient and user-friendly framework, creating an interface that functions fluidly and provides an accessible channel for people to readily engage with the platform.

2. Integrity

Due to its high mean score and prominence in Table 5.1, integrity was given priority, which shifted attention to the advancement of the digital platform. Utilising **Solidity** to create secure smart contracts, the researcher created transparent, automated transactions using blockchain's capabilities. This served as the foundation for features on the Ethereum blockchain, including lodging reservations and centre listings. Additionally, for blockchain integration in the GMS digital platform, **Web3** was used, which is a JavaScript library that allows interaction with the blockchain. Web3 facilitates communication between the platform and users' Ethereum wallets, enabling secure and transparent transactions.

3. Confidentiality

In order to achieve robust confidentiality, **MetaMask**, a technology that is renowned for protecting user information, was used. This technology allows network users to

maintain sole control over their data, establishing a safe atmosphere that respects user privacy inside the platform.

4. Availability

Another essential pillar in strengthening the security of the digital platform is availability. Data from Table 5.1 shows that it is crucial to guarantee continuous user access. To create a decentralised framework, the researcher integrated the distributed file system **Infura IPFS** (InterPlanetary File System), which stores data across numerous nodes. Distributing user data across nodes reduces the danger of illegal access and data loss while enhancing data security and ensuring availability.

5.1.3. Architecture design

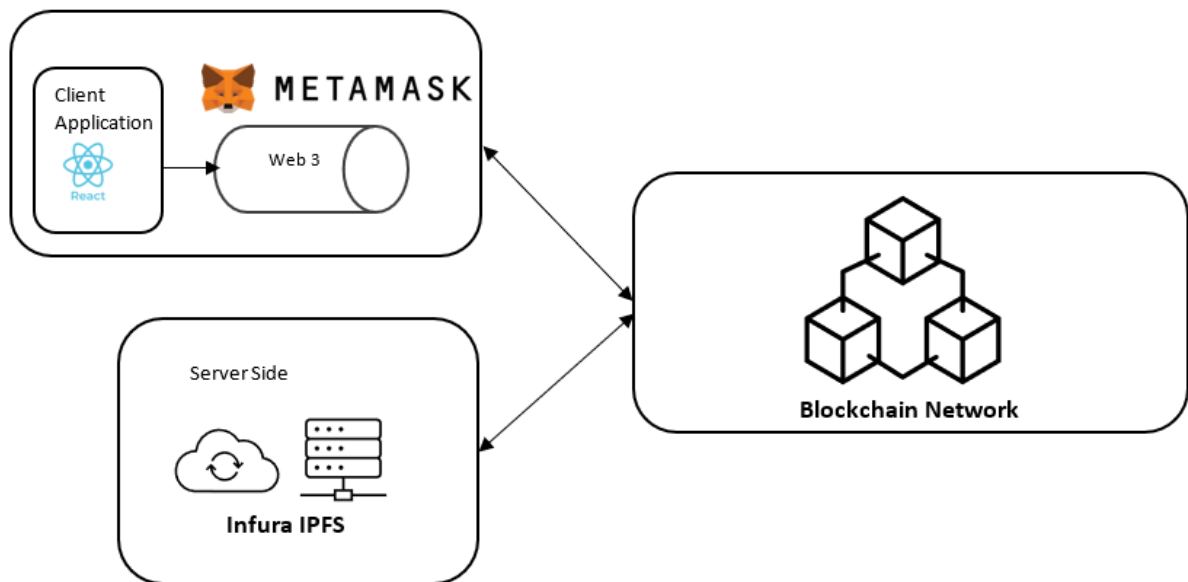


Figure 5.1. GMS decentralised architecture

The architecture of the GMS digital platform is shown in Figure 5.1. It utilises **ReactJS** to create the client-side application. It is available thanks to hosting provided by a distributed network using **Infura IPFS**. With each node storing ledger copies and smart contracts for data security, the back end uses the Ethereum blockchain network to implement a distributed server arrangement. Utilising smart contracts for frictionless transactions and **MetaMask** for secure authentication, the application runs on the Ethereum platform. This integration of technologies ensures both user convenience and data security.

5.1.4. System design

5.1.4.1. Authentication flow chart

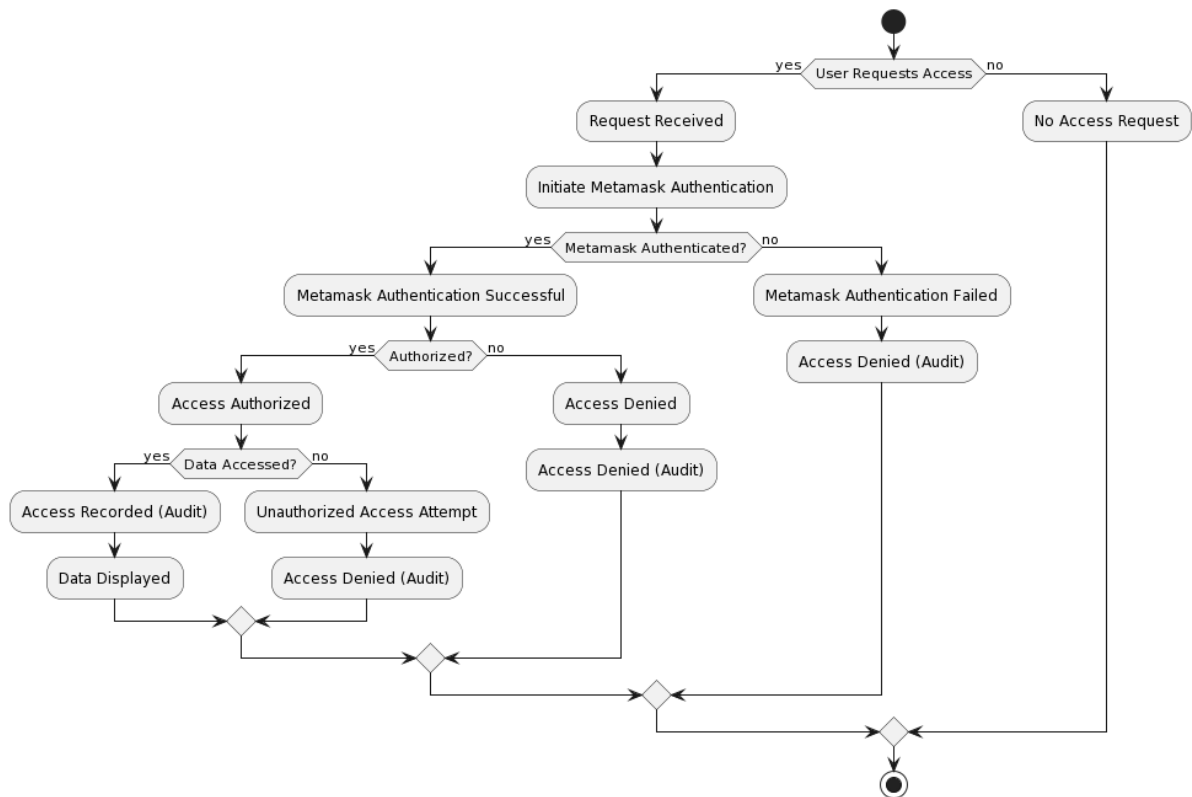


Figure 5.2. Authentication flowchart

This flowchart clearly illustrates the user's access journey and aligns with the CIA Triad's confidentiality component, as shown in Figure 5.2. MetaMask performs authentication to confirm their identity in response to the user's request. After successful authentication, access to the data is determined by the verification of authorisation. Data is displayed, and auditing is started when authorisation is received. Access is denied, and unauthorised access attempts prompt auditing. Access is prohibited, and a failure is logged if MetaMask authentication fails. The flowchart embodies the CIA Triad principles and captures the secure data interaction cycle.

5.1.4.2. Data integrity flowchart

The process of safe transactions inside a distributed application is graphically shown in Figure 5.3. Transactions are started by users and approved by MetaMask. Smart contracts carefully validate valid transactions, assuring non-repudiation. Blockchain stores the transaction after confirmed integrity and is protected against tampering.

Whether successful or not, confirmations uphold openness and user confidence and represent the application's dedication to solid data security.

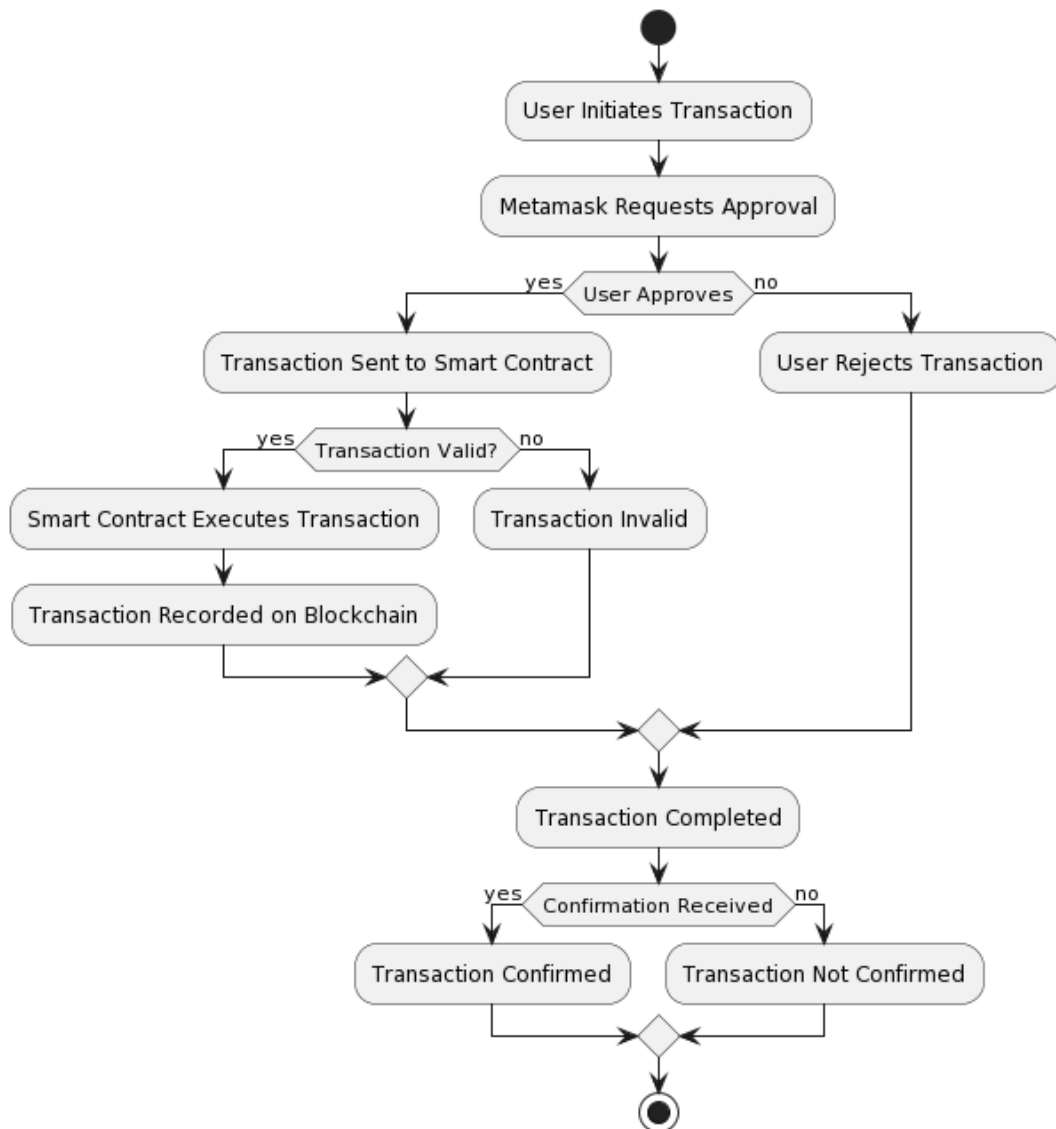


Figure 5.3. Data integrity flowchart

5.1.4.3. Availability flowchart

Figure 5.4 shows the key component of data availability within the CIA Triad. The procedure starts with a user creating a distinct hash and putting data on IPFS. The data is then shared or saved as a hash of this representation. The hash is employed when a user requests data to quickly get and show the requested data from IPFS. This simplified procedure illustrates IPFS's contribution to data accessibility while upholding the CIA Triad's guiding principles.

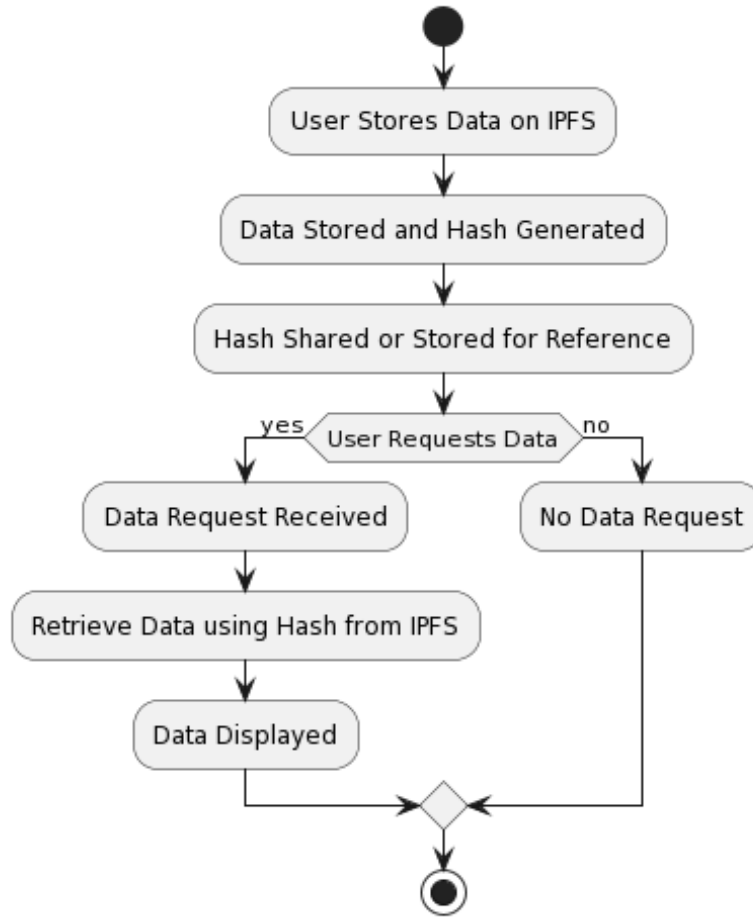


Figure 5.4. Availability flowchart

5.1.4.4. Use case scenario

Within this use case's GMS digital platform, Father John Doe and Sister Mary represent the roles of host and visitor, respectively. Father John Doe uses his MetaMask wallet to secure Ethereum blockchain identification and registers his mission centre. Following suit, Sister Mary uses the "Accommodation" module of the platform to find suitable lodging, relying on the blockchain's transparency and specially designed services for Catholic missionaries in the area. Sister Mary makes the most of the platform's potential throughout her stay, using it to arrange accommodation and establish links with other Catholic missionaries. Interactions are more trustworthy because every transaction is secure and traceable because of the platform's blockchain core. Because it incorporates cutting-edge blockchain technology and features specifically designed to meet the unique needs of Catholic missionaries in the region, the Global Mission Services digital platform offers a decentralised and safe channel for missionaries like Father John Doe and Sister Mary.

5.1.4.5. Use case diagram

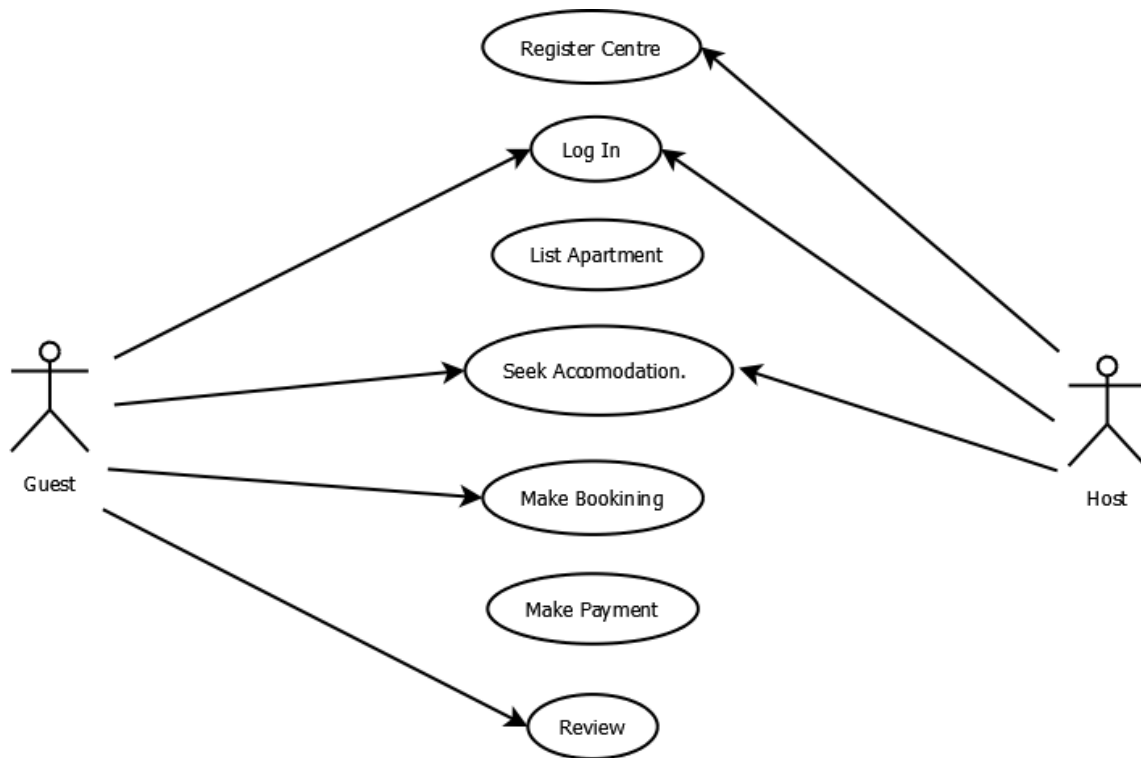


Figure 5.5. GMS use case diagram

5.1.4.6. The sequence diagram

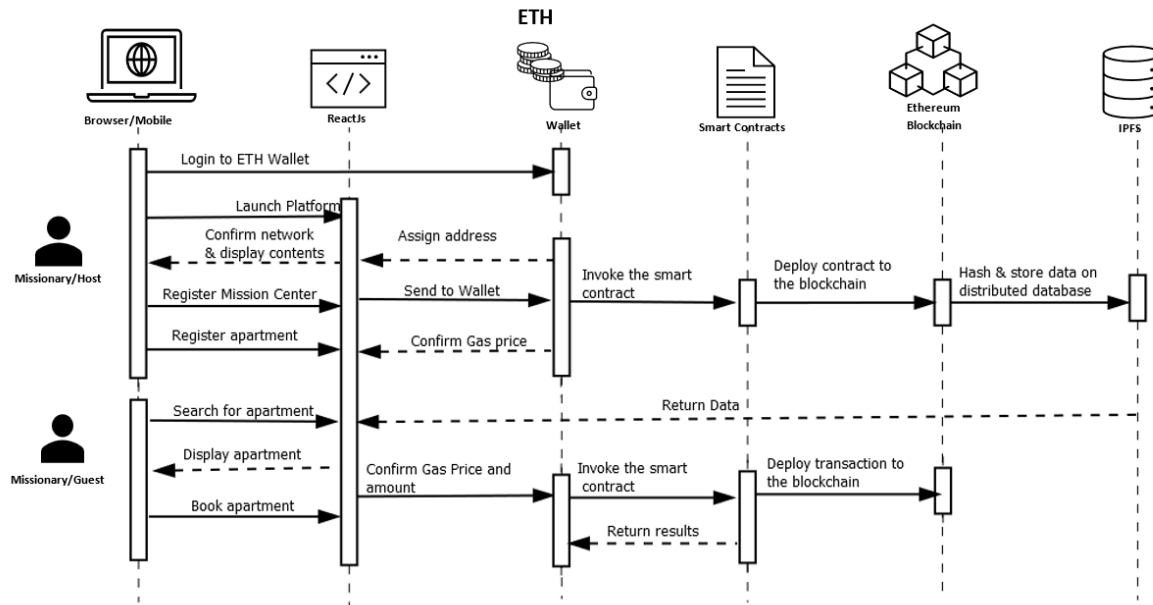


Figure 5.6. Sequence diagram of GMS digital platform

This section clarifies the sequence diagram involving numerous actors, including users (hosts or guests), the Ethereum blockchain, IPFS, the mobile app, ReactJS, the smart contract, and users (hosts or guests) of the Ethereum wallet MetaMask. A sequence diagram in Figure 5.6 depicts the information flow's chronological order. Users (missionaries) log into their MetaMask Ethereum wallets through the mobile app to get an authentication address, which starts the process. Use of the digital platform powered by ReactJS begins after logging in. Users can register businesses or list residences, which causes ReactJS to send requests for transaction amounts and gas price validation to the Ethereum wallet. The smart contract activates after confirmation, analysing registration or listing data and indicating success or failure.

For apartment reservations, users use ReactJS to query IPFS for pertinent information, and then they choose their accommodations and send requests. This starts a chain of events: the ReactJS front end informs the Ethereum wallet of the transaction and gas details, which initiates the smart contract. Acceptance or rejection of a transaction is based on its results, with successful bookings being hashed and stored on the Ethereum blockchain. Through their Ethereum wallets, users may keep up with transaction results, and using the logout option puts an end to their interaction.

5.1.4.7. Class diagram

Figure 5.7 illustrates the four fundamental classes that make up the prototype: Centre, Accommodation, Guest, and Host.

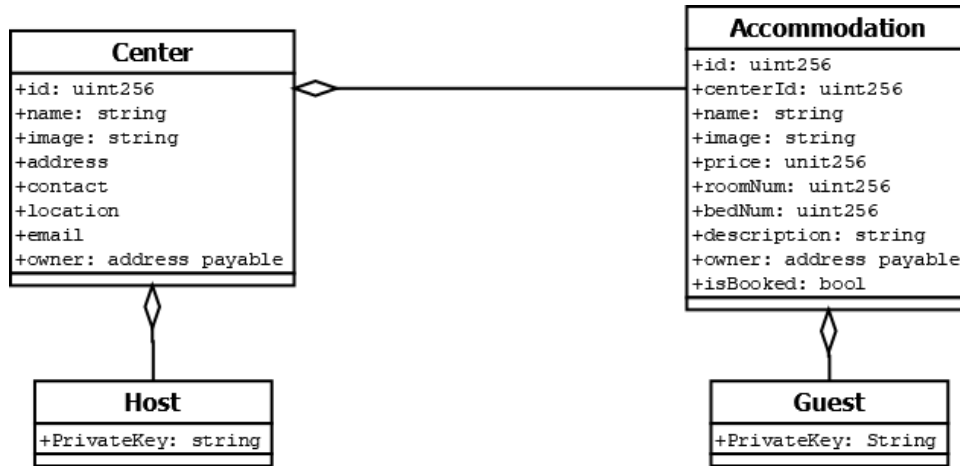


Figure 5.7. Class diagram

The classes for the "Center," "Accommodation," "Host," and "Guest" smart contracts are part of the Global Mission Services (GMS) platform's class diagram, which is depicted in Figure 5.7. The graph displays relationships between "Accommodation" and the "Host" and "Guest" classes as well as one-to-many links between "Center" and "Accommodation". Even while every "Accommodation" links to a single "Center", each "Center" can also link to several "Accommodations". The GMS platform also enables multiple "Hosts" and "Guests" to be connected to a single "Accommodation", enabling sophisticated interactions.

5.1.5. Prototype implementation

This section describes the hardware and software components needed to assemble the prototype. It also describes the smart contracts, the prototype environment, and the execution of the prototype. After reading this section, the reader should be able to set up the development environment and run the prototype.

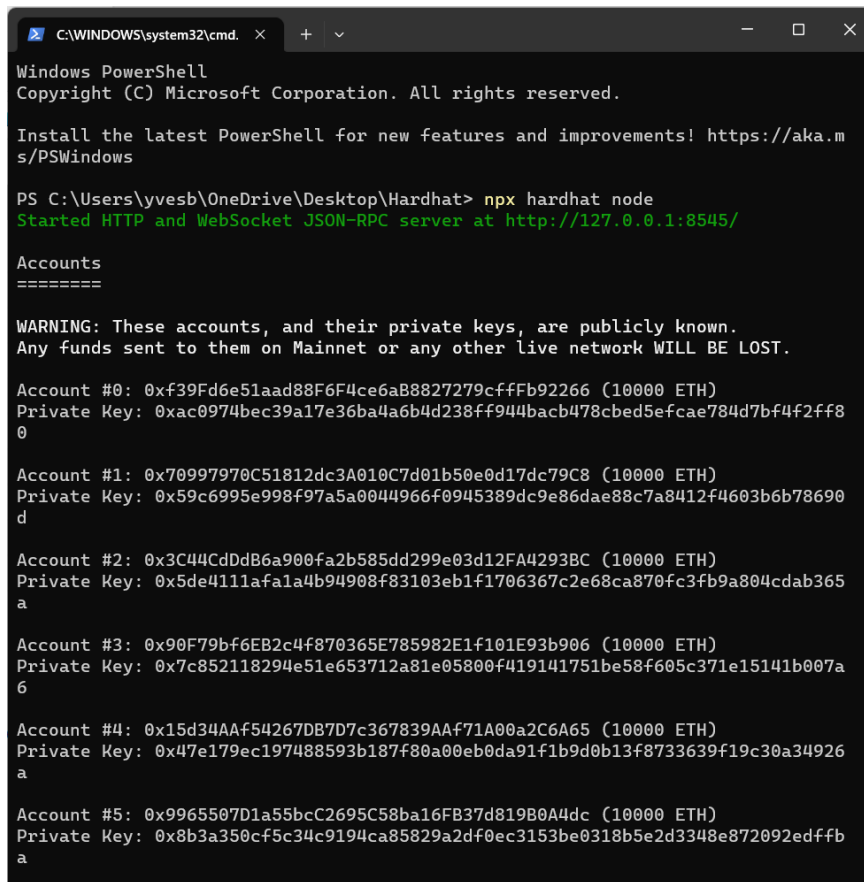
5.1.5.1. Hardware component

The prototype was created on a laptop with an i5 Core processor, 8 gigabytes of RAM, and a 250 gigabyte Solid State Drive (SSD), which provided an adequate balance of processing power, memory, and storage capacity for the project's development requirements.

5.1.5.2. Software component

The front end was developed in ReactJS. The back end was developed in Solidity and the testing framework used was Hardhat and Infura IPFS for distributed storage.

To start the Hardhat server, the first step is to open a terminal and navigate to the project directory. Next, run “npx hardhat node” to start a local Ethereum network. This will create 20 test accounts with 10,000 ETH each, and provide you with a URL for your local blockchain node. Keep this terminal window open to keep the network running. The created accounts are shown in Figure 5.8.



```

C:\WINDOWS\system32\cmd. x + v
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\yvesb\OneDrive\Desktop\Hardhat> npx hardhat node
Started HTTP and WebSocket JSON-RPC server at http://127.0.0.1:8545/

Accounts
=====

WARNING: These accounts, and their private keys, are publicly known.
Any funds sent to them on Mainnet or any other live network WILL BE LOST.

Account #0: 0xf39Fd6e51aad88F6F4ce6aB8827279cFfFb92266 (10000 ETH)
Private Key: 0xac0974bec39a17e36ba4a6b4d238ff944bacb478cbed5efcae784d7bf4f2ff80
0

Account #1: 0x70997970C51812dc3A010C7d01b50e0d17dc79C8 (10000 ETH)
Private Key: 0x59c6995e998f97a5a0044966f0945389dc9e86dae88c7a8412f4603b6b7690d
d

Account #2: 0x3C44CdDdB6a900fa2b585dd299e03d12FA4293BC (10000 ETH)
Private Key: 0x5de4111afa1a4b94908f83103eb1f1706367c2e68ca870fc3fb9a804cdab365a
a

Account #3: 0x90F79bf6EB2c4f870365E785982E1f101E93b906 (10000 ETH)
Private Key: 0x7c852118294e51e653712a81e05800f419141751be58f605c371e15141b007a
6

Account #4: 0x15d34AAf54267DB7D7c367839AAf71A00a2C6A65 (10000 ETH)
Private Key: 0x47e179ec197488593b187f80a00eb0da91f1b9d0b13f8733639f19c30a34926a
a

Account #5: 0x9965507D1a55bcC2695C58ba16FB37d819B0A4dc (10000 ETH)
Private Key: 0x8b3a350cf5c34c9194ca85829a2df0ec3153be0318b5e2d3348e872092edffba
a

```

Figure 5.8. Hardhat local server accounts

To import the ETH to the MetaMask wallet, open MetaMask wallet and switch to the network where the local Ethereum node was started (usually “Localhost 8545”). Click on “Add Token” and enter the contract address, along with the token symbol and decimal places for your contract. Then click on “Next” followed by “Add Tokens” to add the contract to your MetaMask wallet. The MetaMask wallet is shown in Figure 5.9.

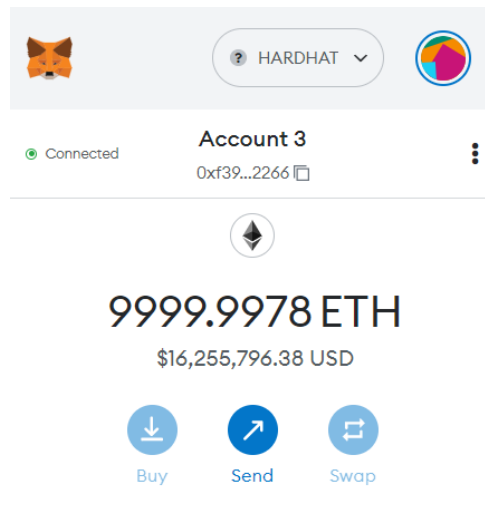


Figure 5.9. MetaMask account

After setting up the Hardhat testing server and the wallet, the next step is to compile, test and deploy the contracts. By running the comment “npx hardhat compile”, “npx hardhat test” and “npx hardhat deploy” respectively.

Below are two of the contracts that were created for the purpose of this prototype, namely Accommodation and Mission contracts written in Solidity programming language.

```

C:\WINDOWS\system32\cmd. x + v
Contract deployment: Mission
Contract address: 0x5f8db2315678afecb367f032d93f642f64180aa3
Transaction: 0xb9c0848e28bb4563341532556584a950b715e1292b6c4c34093eb7aef928e21
From: 0xf39fd6e51aad88f6f4ce6ab8827279cfff92266
Value: 0 ETH
Gas used: 1394756 of 1394756
Block #1: 0xdb470245e4988a436ec86d30a5efd93091082e45c33be4e1f81c311abedb3bc1

eth_chainId
eth_getTransactionByHash
eth_chainId
eth_getTransactionReceipt
eth_accounts
eth_chainId
eth_estimateGas
eth_feeHistory
eth_sendTransaction
Contract deployment: Accommodation
Contract address: 0xe7f1725e7734ce288f8367e1bb143e90bb3f0512
Transaction: 0xee2315692a46a4564042f0982bf4890a70ce73c743944c14dc94b5354a9b65f8
From: 0xf39fd6e51aad88f6f4ce6ab8827279cfff92266
Value: 0 ETH
Gas used: 1300226 of 1300226
Block #2: 0xeb8c40cdf343e14749dbb385d7835abe08cb7b462c54781f88a5539210bad78

eth_chainId
eth_getTransactionByHash
eth_chainId
eth_getTransactionReceipt

```

Figure 5.10. Deployed contract information

5.1.5.2.1. Font-end design

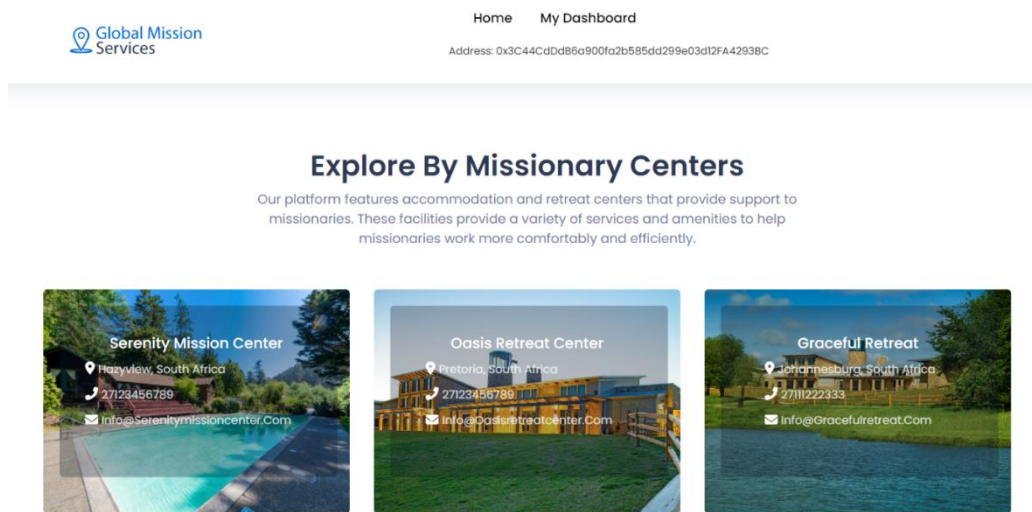


Figure 5.11. GMS home page, missions section

The home page of the GMS digital platform is shown in Figure 5.11. Missionaries mainly use the platform for advertising and highlighting their facilities, such as residences and retreat facilities. The figure shows the platform's highlighted mission locations in South Africa and the Kingdom of Eswatini. Name, address, and other crucial details about each centre are displayed succinctly and simply. Users can choose the desired mission centre by simply navigating the list of mission centres. On the home page, the user's Ethereum address is visible. This address controls transactions and keeps tabs on user platform usage. Because it enables users to conduct transactions with one another securely and openly, the Ethereum address is an essential part of the platform.

5.2. Data Security Evaluation

The evaluation of the framework and testing of the prototype were completed during this phase. The evaluation's goal was to determine whether the framework can ensure data security on digital platforms, which was proven by creating a distributed application that runs on the Ethereum network. This prototype has been tested to determine how closely the application adheres to the CIA Triad's three guiding principles. The tests that were conducted, the results obtained, and the suggestions made are all described in this report.

5.2.1. Testing procedures

The test was conducted in stages. The prototype was tested to see whether it ensures strong authentication, authorisation, and availability as part of the first phase of evaluating the framework's confidentiality component. Testing the prototype's integrity made up the second stage. One of the crucial components of the testing procedure was that Smart contracts were one of the blockchain's components that ensured integrity. At this point, smart contracts were tested on the Hardhat local development network and the Polygon Infura Ethereum network to see whether they complied with all data integrity criteria. Finally, it was uploaded to a distributed database called IPFS to evaluate the system's availability.

5.2.1.1. Confidentiality evaluation

5.2.1.1.1. Authentication

The platform differs between two different user categories: hosts and guests. The platform's authentication system depends on MetaMask, as was previously mentioned. The resilience of MetaMask's ability to establish, preserve, and use cryptographic key pairs was eventually confirmed after this authentication process received careful examination in a battery of demanding tests. As a result, a solid basis for secure user authentication was created within the distributed application. In this system, using users' private keys is crucial for user identification. The capacity of MetaMask to produce strong key pairs for hosts and visitors has been continuously shown through methodical testing techniques. Notably, these keys are stored safely inside users' devices within MetaMask. This strengthens the security of cryptographic assets, protecting the information against illegal access. Additionally, users could regain account access in cases like device loss thanks to the mnemonic phrase backup functionality, which has now established itself as a reliable tool.

Integrating the MetaMask authentication framework with the decentralised application (DApp) conception flowed smoothly. Thorough testing confirmed the efficient use of private keys for transaction signing. This procedure results in digital signatures that can be trusted implicitly to vouch for the truthfulness and integrity of the relevant

transactions. Referentially, Figure 5.12 graphically represents the private key produced by MetaMask's methods.

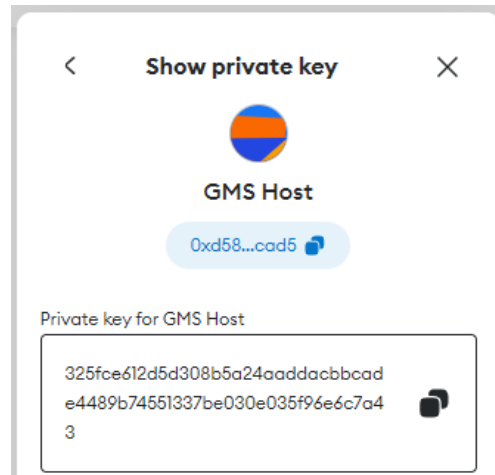


Figure 5.12. Private key generated by MetaMask

5.2.1.1.2. Authorisation

In this section, the main aim was to evaluate the efficacy of the authorisation protocols associated with MetaMask within the context of the GMS digital platform. The core of the investigation revolved around the extent to which these limitations orchestrated the landscape of data visibility and user access within the platform's framework. The testing confirmed the effective integration of MetaMask's smart contract-based Ethereum authorisation. A distinct Ethereum address was given to each registered host and visitor, serving as their secure credential. Using MetaMask, which safely communicated Ethereum addresses to the platform's back end, the testing proved that hosts and visitors could log in without any issues. Authorised hosts and guests were successfully granted access to their specific dashboards through the smart contract validation process.

The registration process for hosts appeared to be simple during testing. Hosts could efficiently handle the data in their centre once they had registered and had access to their personal dashboards. With the aid of public-private key pairs from MetaMask, a robust authentication procedure was made possible, ensuring secure access to sensitive data. The host profile is shown in Figure 5.13. Each user has a unique address that grants them access to the information they are authorised to view.

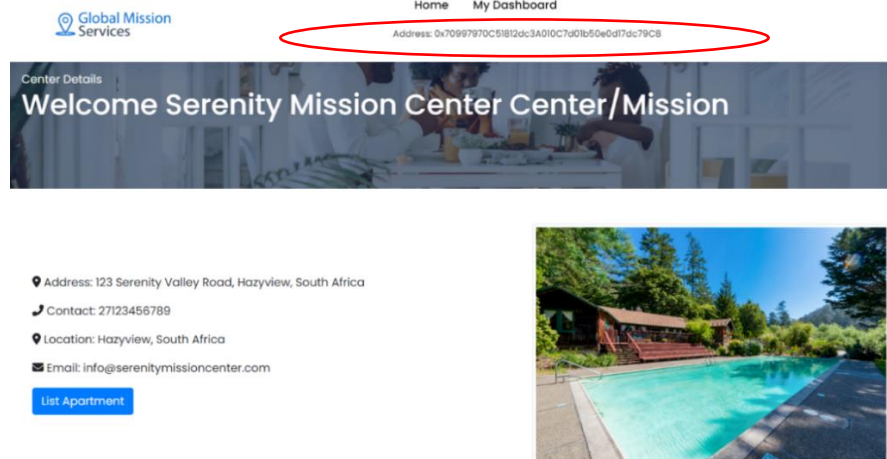


Figure 5.13. Mission Dashboard/Centre Profile

The testing demonstrated the effective use of role-specific access controls for guests. Guests were limited to making and managing reservations, and because of MetaMask's cryptographic features, their access was restricted to the necessary information. This strategy improved security and reduced unnecessary exposure by ensuring that users only dealt with the data relevant to their tasks. Figure 5.14 shows the user's booking page.

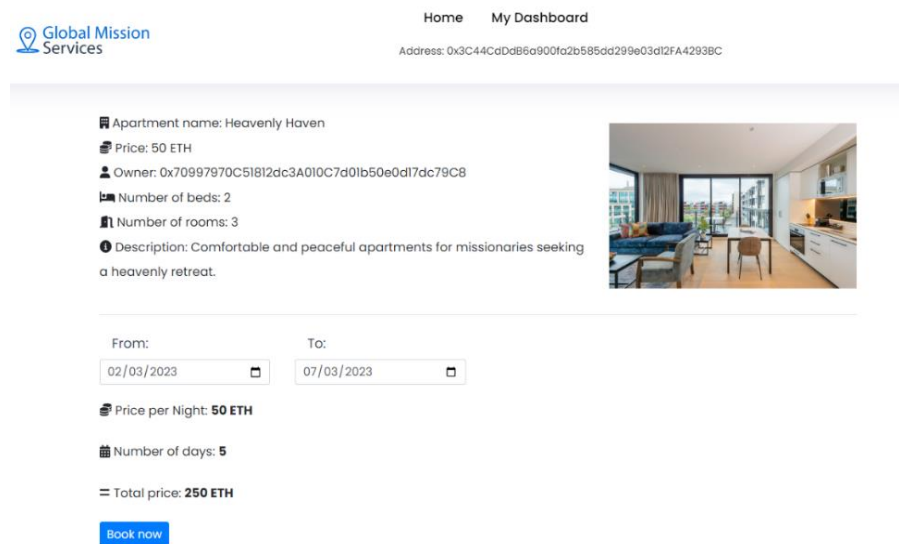


Figure 5.14. Booking page

The researcher verified the synchronisation between data visibility and specific centres only for hosts, with the sole privilege for them to initiate bookings, by putting the system through a variety of test scenarios. The platform was created to enable hosts to efficiently manage the data for their centres while also enabling guests to make booking decisions and keep an eye on reservations related to their information. The

effectiveness of MetaMask's permission mechanism was highlighted by this evaluative technique, which successfully thwarted all attempts to access data without authorisation.

5.2.1.1.3. Accountability

In order to guarantee transparent and tamper-proof user data and activities throughout testing, the accountability and audit procedures excelled. The technology ensured a reliable method for monitoring and verifying user interactions by drawing on MetaMask's cryptographic capabilities and the blockchain's immutability. We looked at how MetaMask's blockchain integration and cryptographic signatures recorded user behaviours during the testing phase. Each user transaction has a distinctive digital signature created with their private key and is safely preserved on the blockchain. A trustworthy audit trail was created by this method, which time-stamped and tracked user actions. Due to the decentralised, tamper-proof structure of the blockchain and the cryptographic methods used by MetaMask, attempts to alter records were unsuccessful.

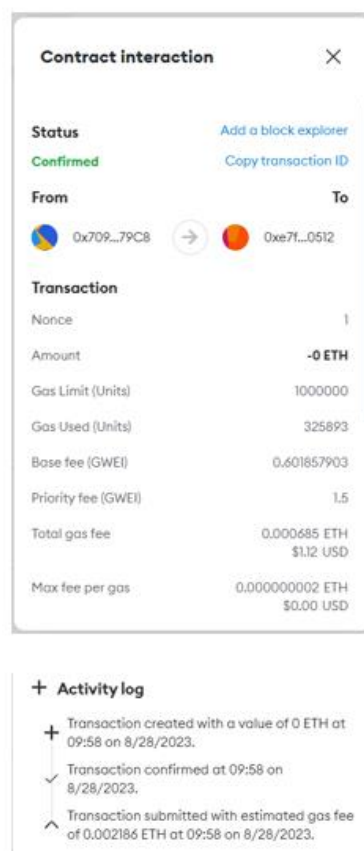


Figure 5.15. Transaction details and activity log

Figure 5.15 shows transaction information, such as the total amount, gas used, fees, and cost, providing specifics on particular user interactions. The activity log with this document creates a thorough and chronological record of user interactions. These measures improve transparency and accountability by accurately recording and verifying user behaviours.

5.2.1.2. Integrity evaluation

Due diligence and rigorous testing were performed on the smart contract code due to the platform's integrity commitment. Assessing security and performance and ensuring resilience were among the steps. By installing contracts on Ethereum for testing, new information about local network deployment was revealed. This information specifies contract addresses, transactions, and gas usage, providing essential elements for decentralised apps.

5.2.1.2.1. Smart contract testing local network

Initially, a robust development tool called Hardhat was used to examine the smart contract code in a controlled environment. The researcher could carefully assess the code's behaviour, interactions, and potential vulnerabilities. The researcher could find and fix problems in a secure environment by exposing the contracts to a regulated local network. The results shown in Figure 5.16, which resulted from the 'npx hardhat test' command being run, were crucial in confirming the dependability of the smart contracts. A stringent testing architecture with extensive test cases was implemented to accomplish this. A key stage in ensuring the accuracy of the contracts' operations, these tests were tactically created to scrutinise data input validation. Beyond ensuring functionality, these tests were crucial in boosting the smart contracts' resistance to threats and vulnerabilities that could be brought about by poor data validation.

```
$ npx hardhat test

Accommodation
  ✓ should create an accitem (154ms)
  ✓ should book an accitem (116ms)

Mission
  ✓ should create a center (111ms)
  ✓ should not create a center without a name (174ms)
  ✓ should not create a center without an image

5 passing (5s)
```

Figure 5.16. Data validation testing results

5.2.1.2.2. Testing and execution of smart contracts online

The researcher expanded the scope of the research to a live Ethereum network, specifically Polygon Infura, building on the knowledge gathered from local testing. This change allowed the researcher to evaluate contract performance and behaviour in a real-world setting. This was done to determine whether the smart contract complied with all standards for blockchain technology. The smart contracts underwent extensive testing and met all requirements established by the blockchain environment. These exacting standards ensured that transactions are conducted with the highest level of security and compliance, supporting the system's overall integrity. The outcomes are displayed in Figure 5.17 and Figure 5.18 for both the mission and accommodation smart contracts.

 **Contract Source Code Verified** (Exact Match) 

Contract Name:	Mission	Optimization Enabled:	No with 200 runs
Compiler Version	v0.8.17+commit.8df45f5f	Other Settings:	default evmVersion, None license

 **Contract Source Code** (Solidity)

VS Code IDE  Beta Outline  More Options

```

1 // **
2 // Submitted for verification at PolygonScan.com on 2023-08-17
3 //
4
5 // SPDX-License-Identifier: MIT
6 pragma solidity ^0.8.0;
7
8 contract Mission {
9     uint256 private _centerIds;
10
11     struct Center {
12         uint256 id;
13         string name;
14         string image;
15         string address;
16         string contact;
17         string location;
18         string email;
19         address payable owner;
20     }
21
22     mapping(uint256 => Center) private _centers;
23
24     event CenterCreated(
25         uint256 indexed id,
```

Figure 5.17. Mission contract verification results

 **Contract Source Code Verified** (Exact Match) 

Contract Name:	Accommodation	Optimization Enabled:	No with 200 runs
Compiler Version	v0.8.17+commit.8df45f5f	Other Settings:	default evmVersion, None license

 **Contract Source Code** (Solidity)

VS Code IDE  Beta Outline  More Options

```

1 // **
2 // Submitted for verification at PolygonScan.com on 2023-08-17
3 //
4
5 // SPDX-License-Identifier: MIT
6 pragma solidity ^0.8.0;
7
8 contract Accommodation {
9     uint256 private _centerId;
10    uint256 private _accitemIds;
11
12    struct Accitem {
13        uint256 id;
14        uint256 centerId;
15        string name;
16        string image;
17        uint256 price;
18        uint256 roomNum;
19        uint256 bedNum;
20        string description;
21        address payable owner;
22        bool isBooked;
23    }
```

Figure 5.18. Accommodation contract verification results

5.2.1.3. Availability evaluation

As an essential component of the framework's performance, the system's availability was thoroughly evaluated as part of the framework evaluation methods. When used in this context, availability refers to a system's capacity to continue operating, being reachable, and responding to user requests, guaranteeing continued service delivery even in the face of potential disruptions. The assessment was based on the white paper released by Fleek Network in (2023). According to the report, two factors ensure that a system will be available. The first one is IPFS integration, and the second is the system's successful deployment on a decentralised edge platform.

5.2.1.3.1. IPFS-Infura integration

By adopting the Infura IPFS (InterPlanetary File System), integration was a strategic step carried out by using APIs within the system developed using React.js. This successful integration was critical in ensuring all uploaded data were securely kept within the IPFS distributed database. The application establishes a strong and dependable connection to the IPFS network using Infura's API endpoints and the associated login credentials.

```
JS ipfs.js > ...
import { create } from 'ipfs-http-client'
const projectId = "2LAjfHsBZfCMYkeMYZKWNxwOjaD";
const projectSecret = "e155ed62f18b48da6d57b61820aeb647";
const auth =
  "Basic " + Buffer.from(projectId + ":" + projectSecret).toString("base64");
const ipfs = create ({
  host: "ipfs.infura.io",
  port: 5001,
  protocol: "https",
  apiPath: "/api/v0",
  headers: {
    authorization: auth,
  },
});
export default ipfs;
```

Figure 5.19. Seamless Integration of Infura IPFS ensures secure and reliable data storage

5.2.1.3.2. System deployment on Fleek Network

The Infura gateway is meticulously configured during deployment to allow seamless interaction between the distributed application and the IPFS network. This intentional integration enables the application to use the vast potential of decentralised data storage. Fleek, known for its expertise in deploying decentralised apps, is the application's host. This option has several advantages, including deploying the application across multiple IPFS nodes, considerably increasing its accessibility and availability to end users. The initial stage in putting the platform online was to design the system using the built-in capability of the Fleek Network. The build process determines whether the system contains defects or errors. Figure 5.20 shows the building log showing the successful build of the GMS digital platform.

```
11:57:02 AM 08/25/2023: The project was built assuming it is hosted at /.
11:57:02 AM 08/25/2023: You can control this with the homepage field in your package.json.
11:57:02 AM 08/25/2023: The build folder is ready to be deployed.
11:57:02 AM 08/25/2023: You may serve it with a static server:
11:57:02 AM 08/25/2023: npm install -g serve
11:57:02 AM 08/25/2023: serve -s build
11:57:02 AM 08/25/2023: Find out more about deployment here:
11:57:02 AM 08/25/2023: https://cra.link/deployment
11:57:03 AM 08/25/2023: Deployed to IPFS and got the hash:
11:57:03 AM 08/25/2023: QmZ6TPmbK4LbMMvYPeBXUvmdxZEWfUGs8k8JI5SKDsQ2
11:57:03 AM 08/25/2023: Checking content availability on IPFS...
11:57:04 AM 08/25/2023: Updating DNS records...
11:57:04 AM 08/25/2023: DNS was updated. You can visit the new site at:
11:57:04 AM 08/25/2023: https://polished-hall-9569.on.fleek.co
```

Figure 5.20. The deployment and testing results

The system was successfully tested and deployed on Fleek live network after a successful build. Figure 5.21 displays the deployed system's success summary, demonstrating how effective the deployment was. The system demonstrates a multi-faceted strategy that satisfies the availability requirement through careful deployment and thorough testing.

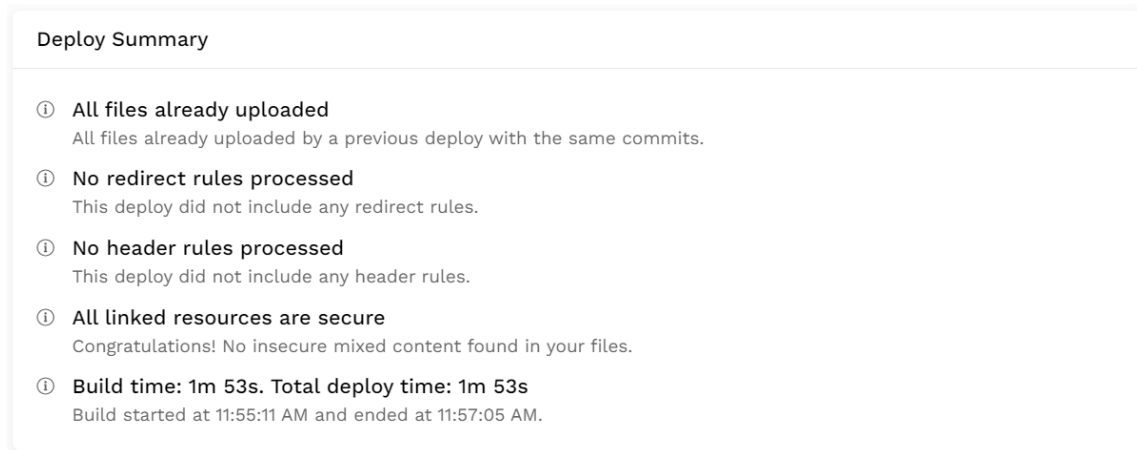


Figure 5.21. Fleek deployment summary

5.3. Summary

The GMS digital platform's data security review produced favourable findings, demonstrating the application's strict adherence to the CIA Triad principles using blockchain technology. The development process was guided by data from a detailed survey. The survey results, which were thoroughly analysed in this chapter, were critical for developing the GMS digital platform to meet the specific preferences and requirements of the missionaries in South Africa and Eswatini. A safe, reliable, and trustworthy user experience was made possible by the MetaMask authentication system, smart contract integrity controls, and IPFS Infura integration. Continual monitoring, updates, and proactive security procedures are advised to guarantee the application's data security as it develops and expands, even though no critical vulnerabilities were found during this examination during the deployment.

6. CHAPTER 6: Discussion, Conclusion, and Future Work

6.0. Introduction

The primary objective of this research was to investigate the application of blockchain technology for data security, using Global Mission Services' (GMS) digital platform as a case study. The comprehensive review of current literature in Chapter 2 highlighted the potential benefits of blockchain technology in strengthening data security while also noting the challenges faced by missionaries in South Africa and Eswatini in preserving data security on their platform. Integrating blockchain technology within the GMS digital platform can potentially increase data security due to its inherent properties, including transparency, immutability, and decentralisation. This was determined based on the obtained findings. Appropriate data collection tools were used, and the data collection process as well as analysis and protocol were followed throughout the research as highlighted in Chapter 3. In Chapter 4, the study also highlighted the techniques used to develop the blockchain technology framework for data security and, in Chapter 5, the GMS prototype development and evaluation were presented. As a result, this chapter brings the study to a close by emphasising the research contributions, reflection, lessons learned, future directions, and final remarks.

6.1. Significant findings

The significant findings of the research are detailed in Table 6.1, outlining the summary of key results obtained from both the survey and the literature review. These points elaborate on important insights into the study through a general overview of the research outcomes.

Table 6.1. Significant findings

Findings	Description
1. Missionaries' activities and geographical focus	The first significant finding of this research is the geographical concentration of missionary centres, as the majority of the centres are in South Africa and a minority in Eswatini. These centres offer diverse services, such as workshops and retreats, for religious, leisure, and business purposes.
2. Digital integration of missionary centres	The study emphasises the need for an online presence, as most centres have websites. Integrating missionary activities into a digital platform is seen as a strategic approach to offer a solid foundation for key services while also addressing long-standing service delivery difficulties.
3. Privacy concerns in digital platforms	The privacy concerns associated with storing sensitive missionary data in the cloud highlight a potential vulnerability. This finding emphasises the critical need for a robust solution to ensure data security and confidentiality, particularly considering the nature of the services provided.
4. Blockchain as a solution	A progressive approach is demonstrated by the introduction of blockchain technology as an innovative way to handle privacy problems. According to the research, the GMS digital platforms may benefit from a secure and reliable environment provided by blockchain technology. Based on the conducted study, the results show how blockchain can enhance data security by guaranteeing confidentiality, integrity and availability.
5. Research gaps in blockchain applications	The potential for further study and improvement is indicated by the discovery of gaps in real-world applications, particularly in security frameworks for digital platforms. Eliminating these shortcomings could improve blockchain systems' efficacy and usefulness in a variety of contexts.

6.1. Reflection

The focus of this study's reflection is on investigating blockchain technology's potential for data security inside a service-based digital platform, with a particular emphasis on the digital platform of GMS. Throughout the investigation, several important conclusions and thoughts have developed. This section describes the three categories of reflection – scientific, substantive, and methodological – relating to the study conclusions. According to Vaishnavi and Kuechler (2004), reflection is a DSR process that is carried out before a research investigation is finished. Scientific reflection entails generalising the research contributions made; substantive reflection establishes the study's purview, while methodological reflection establishes the model-development research procedure.

6.1.1. Scientific reflection

The scientific reflection focuses on the study's contributions to the body of current knowledge and its consequences for the industry. One of the interesting conclusions is the acknowledgement of missionary activities' important role in community development and the difficulty of the lack of readily available information about these services. This information gap is addressed, and services are made more visible by the study's suggestion to combine missionary services into a single digital platform. The significance of technology in closing these gaps and improving access to valuable services is highlighted by this scientific reflection.

The study also highlights the urgent need for strong data security procedures, especially in missionary organisations. The research examines the potential of blockchain technology as a disruptive development from the fourth industrial revolution by investigating its application for data security. This acknowledgement advances the field of blockchain study and positions it as an applicable option for guaranteeing data confidentiality, integrity, and availability. For both researchers and developers, the study's assessment of the benefits of utilising blockchain for data security offers insightful information.

6.1.2. Substantive reflection

The practical results and issues raised by the study are the main subjects of the substantive reflection. The study firstly emphasises how vulnerable sensitive data is to cyber threats, with frequent and costly data breaches. This contemplation emphasises how crucial it is to implement cyber security measures, particularly for groups like missionaries that work for the good of society. The study's recommendation to use blockchain technology to secure private information demonstrates a serious assessment and understanding of the necessity to protect data and reduce risk. Additionally, the case study of the GMS digital platform offers useful perceptions of the effectiveness of applying blockchain technology in practical settings. This thorough reflection presents concrete evidence and experiences that may guide decision-making and implementation strategies for enterprises considering adopting blockchain for data security.

6.1.3. Methodological reflection

The research methodology used in the study makes up the main topics of the methodological reflection. It emphasises the study's dependence on a case study methodology, notably looking at the development of the blockchain framework and the GMS digital platform. This methodological decision enabled a thorough investigation of the possibilities of blockchain technology within a particular environment, offering complex insights into its efficacy and difficulties. The methodological reflection emphasises the value of empirical research to support theoretical ideas and exemplifies the study's relevance to real-world situations.

Additionally, a thorough review of blockchain technology's effectiveness was used in the study's data security assessment within the service-based digital platform. This methodical perspective recognises the importance of evaluating data confidentiality, integrity, and availability. The study offers a solid basis for understanding the potential of blockchain technology in guaranteeing data security within service-based digital platforms by utilising a detailed methodology.

6.2. Lessons Learned

Throughout this study, the researcher learnt the following:

1. The study emphasised the significance of information accessibility in ensuring the visibility and the use of essential services. The realisation of the information gap in missionary services underlined the need for digital platforms to combine and coordinate all their services. This course emphasises using technology to enhance access to essential services and close knowledge gaps.
2. The study emphasises how vulnerable sensitive data is to cyber threats and how expensive data breaches are. The report highlighted the urgent need for data security and the substantial costs associated with data breaches. This illustrated how crucial it is for organisations handling sensitive data, including missionary services, to implement robust data security protocols. The main lesson is the importance of prioritising and investing in data security solutions to protect sensitive information from cyber-attacks.
3. The study investigated the use of blockchain technology as a disruptive solution for data security on a service-based digital platform. The study identified blockchain as a disruptive development from the fourth industrial revolution by assessing how well it protects data confidentiality, integrity, and availability. The key finding is that blockchain technology can transform current data security procedures completely and ought to be taken into account to boost data integrity and trust inside digital platforms.
4. Another lesson learnt in this study is the importance of empirical research. The study employed a case study methodology to analyse the efficacy of blockchain technology in a specific context. The beneficial knowledge and experiences gained from this empirical investigation informed decision-making and implementation strategies. The major conclusion is the importance of conducting empirical research to support theoretical theories and comprehend the real-world implications of cutting-edge technologies such as blockchain.

6.3. Future Considerations

The current study has made significant progress in investigating the possible value of blockchain technology in strengthening data security within a service-based digital platform created for missionaries. However, it is critical to recognise that this research has fundamental limitations, encouraging the development of other areas for future investigation. These emerging aspects broaden the scope of the continuing inquiry, allowing for additional expansion and progression:

1. **Scalability and performance optimisation:** Although the study successfully illustrated how blockchain was integrated into the GMS digital platform, further research towards improving scalability and performance is encouraged. This will allow it to adapt smoothly to more users without affecting the platform's efficiency.
2. **User experience enhancement:** While the security aspects of digital platforms are highlighted in this study, the importance of the user experience should not be understated. Future research might improve user experience through usability tests, gathering user feedback, and gradually improving the platform's interface and functionality.
3. **Regulatory and legal frameworks:** As blockchain technology progresses, so do the regulatory and legal issues surrounding its application. Future considerations should thoroughly examine key legal frameworks, data privacy rules, and compliance requirements to guarantee that the platform meets industry standards.
4. **Keeping pace with technological developments:** Continuous monitoring and studying of blockchain technology's improvements are essential, given that it is continually changing. In order to ensure that recommendations and conclusions are still applicable and up-to-date, future research should continue to be aware of fresh developments, scientific advances, and changes in blockchain.

6.4. Concluding Remarks

This study aimed to investigate the feasibility of using blockchain technology to develop a robust data security framework for missionaries' travel-logistic digital platforms in Eswatini and South Africa. This was achieved firstly, by carrying out an extensive review of available literature on Blockchain technology; secondly, by developing a blockchain framework following the CIA Model to provide data security for service-based digital platforms for missionary travel-logistic services; and thirdly, by testing and implementing the developed Blockchain framework on the GMS digital platform.

The findings of this study provide practical techniques for enhancing data security on missionaries' travel-logistic digital platforms in South Africa and Eswatini. This can also be implemented in different setups in developing countries.

Drawing on the findings of this research study it can be concluded that Blockchain technology can be used to overcome the limitations of traditional data security methods; by improving security through decentralisation, immutability, consensus mechanisms, smart contracts, and transparency.

Table 6.2 summarises the research questions, answers, and evidence.

Table 6.2. Research questions, answers, and evidence

Research question	Answer	Evidence
What are the benefits of implementing a digital platform for Global Mission Services?	According to this research study's findings, the benefits of implementing the GMS digital platform include improving the efficiency of travel logistics and making missionaries' services more readily accessible, resulting in enhanced efficiency and productivity.	Chapter 2, section 2.1; Chapter 5, section Error! Reference source not found..1
How has blockchain technology transformed the technology industry?	The study found that blockchain technology has completely transformed the tech industry through improving data security, transparency, and decentralisation. By introducing secure transactions and smart contracts, its tamper-resistant records redefined conventional data management. Securing data in service-based digital platforms is also a part of this transformational potential.	Chapter 2, section 2.4; Chapter 5, section 5.1.2
To what extent is blockchain technology effective for developing a data security framework?	This study emphasised blockchain's potential for use in creating data security frameworks. Its distributed design, immutability, and consensus mechanism result in a robust and impenetrable security framework. The GMS digital platform prototype demonstrated how data security is improved by blockchain, increasing trust among users and stakeholders.	Chapter 2, sections 2.4.6, 2.4.7 and 2.4.8; Chapter 4; Chapter 5

In this study, the researcher achieved all the objectives. The proposed blockchain framework for data security will assist in improving data security in service-based digital platforms, specifically in the missionaries' network in South Africa and Eswatini.

References

- Abhimanyu, S. (2024), "Angular vs React vs Vue: Which One is the Best?", available at: <https://www.scaler.com/blog/angular-vs-react-vs-vue/> (accessed 4 December 2024).
- Adlam, R. and Haskins, B. (2019), "A Permissioned Blockchain Approach to the Authorization Process in Electronic Health Records", *Proceedings - 2019 International Multidisciplinary Information Technology and Engineering Conference, IMITEC 2019*, Institute of Electrical and Electronics Engineers Inc., doi: 10.1109/IMITEC45504.2019.9015927.
- Ahmad, A., Saad, M., Bassiouni, M. and Mohaisen, A. (2018), "Towards blockchain-driven, secure and transparent audit logs", *ACM International Conference Proceeding Series*, pp. 443–448, doi: 10.1145/3286978.3286985.
- Ahmed, S., Soaibuzzaman, Rahman, M.S. and Rahaman, M.S. (2019), "A Blockchain-Based Architecture for Integrated Smart Parking Systems", *2019 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2019*, IEEE, No. March, pp. 177–182, doi: 10.1109/PERCOMW.2019.8730772.
- Alawode, A.O. (2016), "Looking at human development through the lens of Christian mission", *In Die Skriflig/In Luce Verbi*, AOSIS, Vol. 50 No. 1, p. 7, doi: 10.4102/IDS.V50I1.2063.
- Aldweesh, A., Alharby, M., Mehrnezhad, M. and van Moorsel, A. (2021), "The OpBench Ethereum opcode benchmark framework: Design, implementation, validation and experiments", *Performance Evaluation*, North-Holland, Vol. 146, p. 102168, doi: 10.1016/J.PEVA.2020.102168.
- Alhussen, A. and Arslan, E. (2021), "Avoiding data loss and corruption for file transfers with Fast Integrity Verification", *Journal of Parallel and Distributed Computing*, Academic Press, Vol. 152, pp. 33–44, doi: 10.1016/J.JPDC.2021.02.002.
- Ali Khan, J., Raman, A.M., Sambamoorthy, N. and Prashanth, K. (2023), "Research Methodology (Methods, Approaches And Techniques)", *Research Methodology (Methods, Approaches And Techniques)*, San International Scientific Publications, doi: 10.59646/RMMETHODS/040.
- Alyami, F. and Almutairi, S. (2021), "Implementing Integrity Assurance System for Big Data", doi: 10.21203/RS.3.RS-485987/V1.
- Andress, J. (2014), "What is Information Security?", *The Basics of Information Security*, Syngress, pp. 1–22, doi: 10.1016/B978-0-12-800744-0.00001-4.
- Argañaraz, M.C., Berón, M.M., Pereira, M.J.V. and Henriques, P.R. (2020), "Detection of Vulnerabilities in Smart Contracts Specifications in Ethereum

- Platforms”, *DROPS-IDN/13015*, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, Vol. 83, doi: 10.4230/OASICS.SLATE.2020.2.
- Aslam, U., Manzoor, S. and Babar, M.I. (2019), “Systematic Literature Review of Blockchain in Requisites of Big Data and its Applications”, *Journal Of Software Engineering & Intelligent Systems ISSN 2518-8739*, No. September.
- Aydar, M., Ayvaz, S. and Cetin, S.C. (2019), “Towards a Blockchain based digital identity verification, record attestation and record sharing system”, No. June.
- Azaria, A., Ekblaw, A., Vieira, T. and Lippman, A. (2016), “MedRec: Using blockchain for medical data access and permission management”, *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, pp. 25–30, doi: 10.1109/OBD.2016.11.
- Azmi, R., Tibben, W. and Win, K.T. (2018), “Review of cybersecurity frameworks: context and shared concepts”, *Journal of Cyber Policy*, Informa UK Limited, Vol. 3 No. 2, pp. 258–283, doi: 10.1080/23738871.2018.1520271.
- Baars, T. and Spruit, M. (2012), “The SeCA model”, *Security Engineering for Cloud Computing: Approaches and Tools*, IGI Global, pp. 19–35, doi: 10.4018/978-1-4666-2125-1.CH002.
- Balaskas, A. and Franqueira, V.N.L. (2018), “Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges”, *2018 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2018*, IEEE, pp. 1–8, doi: 10.1109/CyberSecPODS.2018.8560672.
- Baybulatov, A.A. and Promyslov, V.G. (2020), “Cybersecurity Assessment Using Delay from Backlog Bound Calculation”, *14th IEEE International Conference on Application of Information and Communication Technologies, AICT 2020 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., doi: 10.1109/AICT50176.2020.9368731.
- Beaman, C., Barkworth, A., Akande, T.D., Hakak, S. and Khan, M.K. (2021), “Ransomware: Recent advances, analysis, challenges and future research directions”, *Computers & Security*, Elsevier Advanced Technology, Vol. 111, p. 102490, doi: 10.1016/J.COSE.2021.102490.
- Berghout, T., Benbouzid, M. and Muyeen, S.M. (2022), “Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects”, *International Journal of Critical Infrastructure Protection*, Elsevier, Vol. 38, p. 100547, doi: 10.1016/J.IJCIP.2022.100547.
- Bhattacharjya, A. (2022), “A HOLISTIC STUDY ON THE USE OF BLOCKCHAIN TECHNOLOGY IN CPS AND IOT ARCHITECTURES MAINTAINING THE CIA TRIAD IN DATA COMMUNICATION”, *International Journal of Applied Mathematics and Computer Science*, Sciendo, Vol. 32 No. 3, pp. 403–413, doi: 10.34768/AMCS-2022-0029.

- Bina, R. (2017), "Blockchain Specialization", *Coursera*, available at: <https://www.coursera.org/specializations/blockchain> (accessed 13 February 2023).
- Bistarelli, S., Mazzante, G., Micheletti, M., Mostarda, L., Sestili, D. and Tiezzi, F. (2020), "Ethereum smart contracts: Analysis and statistics of their source code and opcodes", *Internet of Things*, Elsevier, Vol. 11, p. 100198, doi: 10.1016/J.IOT.2020.100198.
- Bommannavar, P. and Bambos, N. (2011), "Security risk management in computing systems with constraints on service disruption", *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, doi: 10.1109/ICCCN.2011.6005875.
- vom Brocke, J., Hevner, A. and Maedche, A. (2020), "Introduction to Design Science Research", pp. 1–13, doi: 10.1007/978-3-030-46781-4_1.
- Bučko, L. (2013), "Challenges of Missionary Work : Communication , Liberation and Human Development", *Emerging Issues in Social Work and Comunity Health in Subsaharan Africa Versus*, No. June, pp. 1–5.
- Cachin, C., Schubert, S. and Vukolić, M. (2017), "Architecture of the Hyperledger Blockchain Fabric", *Leibniz International Proceedings in Informatics, LIPIcs*, Vol. 70, pp. 24.1-24.16, doi: 10.4230/LIPIcs.OPODIS.2016.24.
- Caggiano, F.J. (2022), "The conversion of the missionary: A journey of the heart' pastoral reflection", <https://doi.org/10.1177/00918296221124039>, SAGE PublicationsSage UK: London, England, Vol. 51 No. 1, pp. 11–18, doi: 10.1177/00918296221124039.
- Casino, F., Dasaklis, T.K. and Patsakis, C. (2019), "A systematic literature review of blockchain-based applications: Current status, classification and open issues", *Telematics and Informatics*, Elsevier, Vol. 36 No. May 2018, pp. 55–81, doi: 10.1016/j.tele.2018.11.006.
- Catak, F.O. (2018), "Two-layer malicious network flow detection system with sparse linear model based feature selection", *Journal of the National Science Foundation of Sri Lanka*, National Science Foundation of Sri Lanka, Vol. 46 No. 4, pp. 601–612, doi: 10.4038/JNSFSR.V46I4.8560.
- Chaitanya, Chk., Reddy, C.N., Vignesh, K.S., Krishna, P.R., Roshini, A. and Swetha, K. (2021), "Enhanced Hash Based Image Steganography Technique to Increase Data Integrity and Confidentiality", *2021 7th International Conference on Advanced Computing and Communication Systems, ICACCS 2021*, Institute of Electrical and Electronics Engineers Inc., pp. 1456–1461, doi: 10.1109/ICACCS51430.2021.9442036.
- Chakravarty, A., Kumar, A. and Grewal, R. (2014), "Customer Orientation Structure for Internet-Based Business-to-Business Platform Firms":, <https://doi.org/10.1509/Jm.12.0442>, SAGE PublicationsSage CA: Los Angeles, CA, Vol. 78 No. 5, pp. 1–23, doi: 10.1509/JM.12.0442.

- Chatterjee, R. and Chatterjee, R. (2018), "An Overview of the Emerging Technology: Blockchain", *Proceedings - 2017 International Conference on Computational Intelligence and Networks, CINE 2017*, No. March 2018, pp. 126–127, doi: 10.1109/CINE.2017.33.
- Chatterjee, S., Sundarraj, R.P. and Dutta, K. (2023), "Editorial Special Issue: Design Science Research in Information Systems and Technology", *IEEE Transactions on Engineering Management*, Institute of Electrical and Electronics Engineers Inc., Vol. 70 No. 3, pp. 803–805, doi: 10.1109/TEM.2023.3235644.
- Chen, H., Pendleton, M., Njilla, L. and Xu, S. (2019), "A Survey on Ethereum Systems Security: Vulnerabilities, Attacks and Defenses", *ArXiv: Cryptography and Security*.
- Chicco, G. (2021), "Data Consistency for Data-Driven Smart Energy Assessment", *Frontiers in Big Data*, Frontiers Media S.A., Vol. 4, p. 683682, doi: 10.3389/FDATA.2021.683682/BIBTEX.
- Christidis, K. and Devetsikiotis, M. (2016), "Blockchains and Smart Contracts for the Internet of Things", *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., Vol. 4, pp. 2292–2303, doi: 10.1109/ACCESS.2016.2566339.
- Cioppi, M., Curina, I., Forlani, F. and Pencarelli, T. (2019), "Online presence, visibility and reputation: a systematic literature review in management studies", *Journal of Research in Interactive Marketing*, Emerald Group Holdings Ltd., Vol. 13 No. 4, pp. 547–577, doi: 10.1108/JRIM-11-2018-0139/FULL/XML.
- Clark, V.L.P. and Ivankova, N. V. (2016), "Mixed Methods Research: A Guide to the Field", *Mixed Methods Research: A Guide to the Field*, SAGE Publications, Inc., doi: 10.4135/9781483398341.
- Cohen, L., Manion, L. and Morrison, K. (2017), "Research Methods in Education", *Research Methods in Education*, Routledge, p. 944, doi: 10.4324/9781315456539/RESEARCH-METHODS-EDUCATION-LOUIS-COHEN-LAWRENCE-MANION-KEITH-MORRISON.
- Crespo-Martínez, I.S., Campazas-Vega, A., Guerrero-Higueras, Á.M., Riego-DelCastillo, V., Álvarez-Aparicio, C. and Fernández-Llamas, C. (2023), "SQL injection attack detection in network flow data", *Computers & Security*, Elsevier Advanced Technology, Vol. 127, p. 103093, doi: 10.1016/J.COSE.2023.103093.
- Creswell, J.W. and Creswell, J.W. (2017), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*.
- D. Lalitha Bhaskari, P.S.G.A.S. (2021), "ETHEREUM BLOCKCHAIN FRAMEWORK FOR HEALTHCARE APPLICATIONS", *INFORMATION TECHNOLOGY IN INDUSTRY*, Auricle Technologies, Pvt., Ltd., Vol. 9 No. 1, pp. 1242–1249, doi: 10.17762/ITII.V9I1.264.
- Dawadi, S., Shrestha, S. and Giri, R.A. (2021), "Mixed-Methods Research: A Discussion on its Types, Challenges, and Criticisms", *Journal of Practical*

- Studies in Education*, Global Talent Academy, Vol. 2 No. 2, pp. 25–36, doi: 10.46809/JPSE.V2I2.20.
- Deng, H., Guo, C., Shen, G., Cui, Y. and Ping, Y. (2023), “MCTVD: A malware classification method based on three-channel visualization and deep learning”, *Computers & Security*, Elsevier Advanced Technology, Vol. 126, p. 103084, doi: 10.1016/J.COSE.2022.103084.
- Duan, C. (2023), “A State-of-the-Art Review of Sharing Economy Business Models and a Forecast of Future Research Directions for Sustainable Development: A Bibliometric Analysis Approach”, *Sustainability* 2023, Vol. 15, Page 4568, Multidisciplinary Digital Publishing Institute, Vol. 15 No. 5, p. 4568, doi: 10.3390/SU15054568.
- Dwivedi, Y.K., Ismagilova, E., Rana, N.P. and Raman, R. (2021), “Social Media Adoption, Usage And Impact In Business-To-Business (B2B) Context: A State-Of-The-Art Literature Review”, *Information Systems Frontiers* 2021 25:3, Springer, Vol. 25 No. 3, pp. 971–993, doi: 10.1007/S10796-021-10106-Y.
- Elisa, N., Yang, L., Chao, F. and Cao, Y. (2020), “A framework of blockchain-based secure and privacy-preserving E-government system”, *Wireless Networks*, Springer US, Vol. 0, doi: 10.1007/s11276-018-1883-0.
- Esposito, C., De Santis, A., Tortora, G., Chang, H. and Choo, K.K.R. (2018), “Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?”, *IEEE Cloud Computing*, Vol. 5 No. 1, pp. 31–37, doi: 10.1109/MCC.2018.011791712.
- Feng, K. and Zhang, J. (2017), “Improving availability and confidentiality of shared data under the multi-cloud environment”, *2017 2nd IEEE International Conference on Cloud Computing and Big Data Analysis, ICCCBDA 2017*, Institute of Electrical and Electronics Engineers Inc., pp. 6–10, doi: 10.1109/ICCCBDA.2017.7951875.
- Ferretti, S. and D’Angelo, G. (2020), “On the Ethereum blockchain structure: A complex networks theory perspective”, *Concurrency and Computation: Practice and Experience*, Vol. 32 No. 12, doi: 10.1002/cpe.5493.
- Fleek Network. (2023), *Fleek Network: Decentralized Edge Platform*.
- Fraser, Sandy. and Chris Robinson. (2004), “Doing research with children and young people”, Sage Publications, p. 59.
- Gad, A.G., Mosa, D.T., Abualigah, L. and Abohany, A.A. (2022), “Emerging Trends in Blockchain Technology and Applications: A Review and Outlook”, *Journal of King Saud University - Computer and Information Sciences*, Elsevier, Vol. 34 No. 9, pp. 6719–6742, doi: 10.1016/J.JKSUCI.2022.03.007.
- Garcia-Alfaro, J., Herrera-Joancomartí, J., Lupu, E., Posegga, J., Aldini, A., Martinelli, F. and Suri, N. (2015), “Data privacy management, autonomous spontaneous security, and security assurance”, *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture*

Notes in Bioinformatics), Vol. 8872 No. September, doi: 10.1007/978-3-319-17016-9.

Gavin Wood. (2014), *Ethereum: A Secure Decentralised Generalised Transaction Ledger*.

Gonzalez, A.J., Gronsund, P., Dimitriadis, A. and Reshytnik, D. (2021), "Information security in a 5G facility: An implementation experience", *2021 Joint European Conference on Networks and Communications and 6G Summit, EuCNC/6G Summit 2021*, Institute of Electrical and Electronics Engineers Inc., pp. 425–430, doi: 10.1109/EUCNC/6GSUMMIT51104.2021.9482499.

Goyal, K. and Kumar, S. (2021), "Financial literacy: A systematic review and bibliometric analysis", *International Journal of Consumer Studies*, John Wiley & Sons, Ltd, Vol. 45 No. 1, pp. 80–105, doi: 10.1111/IJCS.12605.

Gregory, M. (2023), "The Ultimate Ethereum Dapp Tutorial (How to Build a Full Stack Decentralized Application Step-By-Step) | Dapp University", available at: <https://www.dappuniversity.com/articles/the-ultimate-ethereum-dapp-tutorial> (accessed 13 February 2023).

Griswold, A. (2016), "It's time for hotels to really, truly worry about Airbnb — Quartz", available at: <https://qz.com/729878/its-time-for-hotels-to-really-truly-worry-about-airbnb/> (accessed 18 October 2021).

Gurneet Kaur. (2024), "React vs Angular vs Vue: A Detailed Comparison Explained", available at: <https://www.almabetter.com/bytes/articles/the-showdown-reactjs-vs-angularjs-vs-vuejs> (accessed 4 December 2024).

Guttentag, D. (2019), "Progress on Airbnb: a literature review", *Journal of Hospitality and Tourism Technology*, Vol. 10 No. 3, pp. 233–263, doi: 10.1108/JHTT-08-2018-0075.

Halabi, T. and Bellaiche, M. (2018), "A broker-based framework for standardization and management of Cloud Security-SLAs", *Computers & Security, Elsevier Advanced Technology*, Vol. 75, pp. 59–71, doi: 10.1016/J.COSE.2018.01.019.

de Haro-Olmo, F.J., Varela-Vaca, Á.J. and Álvarez-Bermejo, J.A. (2020), "Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review", *Sensors 2020, Vol. 20, Page 7171*, Multidisciplinary Digital Publishing Institute, Vol. 20 No. 24, p. 7171, doi: 10.3390/S20247171.

Hartono, E., Kim, K.Y., Na, K.S., Simpson, J.T. and Berkowitz, D. (2013), "Perceived site security as a second order construct and its relationship to e-commerce site usage", *Advances in Intelligent Systems and Computing*, Springer Verlag, Vol. 206 AISC, pp. 1075–1085, doi: 10.1007/978-3-642-36981-0_102/COVER.

Haryanti, T., Rakhmawati, N.A., Subriadi, A.P. and Tjahyanto, A. (2022), "The Design Science Research Methodology (DSRM) for Self-Assessing Digital Transformation Maturity Index in Indonesia", *Proceedings of the 2022 IEEE 7th International Conference on Information Technology and Digital Applications*,

- ICITDA 2022, Institute of Electrical and Electronics Engineers Inc., doi: 10.1109/ICITDA55840.2022.9971171.
- Hasti, V. (2019), "Data Manipulation- Worse than Data Stolen?", available at: <https://www.ilantus.com/blog/data-manipulation-worse-than-data-stolen/> (accessed 24 February 2023).
- Hevner, A. and Park, J. (2004a), *Design Science in Information Systems Research*.
- Hevner, A. and Park, J. (2004b), *U-CARE View Project Modeling Customer Churn View Project*, Vol. 7.
- Hou, H. (2017), "The application of blockchain technology in E-government in China", *2017 26th International Conference on Computer Communications and Networks, ICCCN 2017*, Institute of Electrical and Electronics Engineers Inc., doi: 10.1109/ICCCN.2017.8038519.
- Jackson-Gordon, R. and Plano Clark, V.L. (2023), "Using a Joint Display for Building Integration in a Sequential Study: Informing Data Collection for a Participatory Second Phase", <https://doi.org/10.1177/15586898231179848>, SAGE PublicationsSage CA: Los Angeles, CA, doi: 10.1177/15586898231179848.
- Johnson, B.R. and Christensen, L. (2014), "Educational Research Quantitative, Qualitative, and Mixed Approaches", edited by HESTER, R., SAGE Publications, Inc, p. 977.
- Johnson, J.L., Adkins, D. and Chauvin, S. (2020), "A Review of the Quality Indicators of Rigor in Qualitative Research", *American Journal of Pharmaceutical Education*, American Association of Colleges of Pharmacy, Vol. 84 No. 1, pp. 138–146, doi: 10.5688/AJPE7120.
- Jøsang, A., Ismail, R. and Boyd, C. (2007), "A survey of trust and reputation systems for online service provision", *Decision Support Systems*, North-Holland, Vol. 43 No. 2, pp. 618–644, doi: 10.1016/J.DSS.2005.05.019.
- Junejo, A.Z., Hashmani, M.A. and Memon, M.M. (2021), "Empirical Evaluation of Privacy Efficiency in Blockchain Networks: Review and Open Challenges", *Applied Sciences 2021*, Vol. 11, Page 7013, Multidisciplinary Digital Publishing Institute, Vol. 11 No. 15, p. 7013, doi: 10.3390/APP11157013.
- Kakralapudi, P.V. and Mahmoud, Q.H. (2021), "A Systematic Review of Blockchain for Consent Management", *Healthcare 2021*, Vol. 9, Page 137, Multidisciplinary Digital Publishing Institute, Vol. 9 No. 2, p. 137, doi: 10.3390/HEALTHCARE9020137.
- Kalia, P. and Paul, J. (2021), "E-service quality and e-retailers: Attribute-based multi-dimensional scaling", *Computers in Human Behavior*, Pergamon, Vol. 115, p. 106608, doi: 10.1016/J.CHB.2020.106608.
- Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y. and Hossain, E. (2017), "Enabling Localized Peer-to-Peer Electricity Trading among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains", *IEEE Transactions on*

- Industrial Informatics*, IEEE Computer Society, Vol. 13 No. 6, pp. 3154–3164, doi: 10.1109/TII.2017.2709784.
- Kang, J.J., Fahd, K. and Venkatraman, S. (2018), “Trusted Time-Based Verification Model for Automatic Man-in-the-Middle Attack Detection in Cybersecurity”, *Cryptography 2018*, Vol. 2, Page 38, Multidisciplinary Digital Publishing Institute, Vol. 2 No. 4, p. 38, doi: 10.3390/CRYPTOGRAPHY2040038.
- Katkova, M.A., Tregubov, V.N., Kapustina, N.V., Yussuf, A.A. and Pilipchuk, N.V. (2020), “Application of Blockchain-Based technology for Smart Transport System”, Vol. 148 No. RuDEcK, pp. 261–267, doi: 10.2991/aebmr.k.200730.049.
- Kebande, V.R., Awaysheh, F.M., Ikuesan, R.A., Alawadi, S.A., Dahman Alshehri, M., Abdelaziz Kerrache, C., Ahmad, F., *et al.* (2021), “A Blockchain-Based Multi-Factor Authentication Model for a Cloud-Enabled Internet of Vehicles”, *Sensors 2021*, Vol. 21, Page 6018, Multidisciplinary Digital Publishing Institute, Vol. 21 No. 18, p. 6018, doi: 10.3390/S21186018.
- Keung, Y.H. (2013), “Basic Principle of Information Security”, *Advances in Robotics & Automation*, OMICS Publishing Group, Vol. 03 No. 03, doi: 10.4172/2168-9695.1000e120.
- Khan, M. and Babay, A. (2021), *Toward Intrusion Tolerance as a Service: Confidentiality in Partially Cloud-Based BFT Systems*.
- King, J. (2013), “Measuring the forensic-ability of audit logs for nonrepudiation”, *Proceedings - International Conference on Software Engineering*, pp. 1419–1422, doi: 10.1109/ICSE.2013.6606732.
- Kumar, G., Saha, R., Rai, M.K. and Kim, T.H. (2018), “Multidimensional Security Provision for Secure Communication in Vehicular Ad Hoc Networks Using Hierarchical Structure and End-to-End Authentication”, *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., Vol. 6, pp. 46558–46567, doi: 10.1109/ACCESS.2018.2866759.
- Lau, F., Rubin, S.H., Smith, M.H. and Trajković, L. (2000), “Distributed denial of service attacks”, *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, Vol. 3, pp. 2275–2280, doi: 10.1109/ICSMC.2000.886455.
- Lazar, J., Feng, J.H. and Hochheiser, H. (2017), “Research methods in human-computer interaction”, p. 534.
- Li, S., Doh, I. and Chae, K. (2016), “A group authentication scheme based on lagrange interpolation polynomial”, *Proceedings - 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2016*, Institute of Electrical and Electronics Engineers Inc., pp. 386–391, doi: 10.1109/IMIS.2016.51.

- Li, X., Jiang, P., Chen, T., Luo, X. and Wen, Q. (2020), "A survey on the security of blockchain systems", *Future Generation Computer Systems*, Vol. 107 No. November 2020, pp. 841–853, doi: 10.1016/j.future.2017.08.020.
- Loewenberg, S. (2009), "Medical missionaries deliver faith and health care in Africa.", *Lancet*, Elsevier, Vol. 373 No. 9666, pp. 795–796, doi: 10.1016/S0140-6736(09)60462-1.
- Macdonald, J. (2021), "The 8 Best Online Travel Agencies of 2021", available at: <https://www.tripsavvy.com/best-online-travel-agencies-4776301> (accessed 17 October 2021).
- Mallik, A. (2018), *Man-In-The-Middle-Attack: Understanding in Simple Words*, *Jurnal Pendidikan Teknologi Informatika*, Vol. 2.
- Maria, L. (2021), "In 2021, what are the most popular blockchain frameworks? | by Maria Lopez | Sep, 2021 | DataDrivenInvestor", available at: <https://medium.datadriveninvestor.com/most-popular-blockchain-frameworks-as-of-the-year-2021-980d18474720> (accessed 13 October 2021).
- Mathew, A.R. (2019), "Cyber security through blockchain technology", *International Journal of Engineering and Advanced Technology*, Vol. 9 No. 1, pp. 3821–3824, doi: 10.35940/ijeat.A9836.109119.
- Maxwell, D. (2014), "The missionary movement in african and world history: mission sources and religious encounter 1 david maxwell", No. 2014, pp. 1–52.
- McBride, T., Townsend, A., Ekstrom, M., Lusty, L. and Sexton, J. (2018), "Data integrity: Recovering from ransomware and other destructive events", *Proceedings - 2018 IEEE Cybersecurity Development Conference, SecDev 2018*, Institute of Electrical and Electronics Engineers Inc., p. 140, doi: 10.1109/SECDEV.2018.00036.
- McKim, C. (2022), "Validity: Criterion, Concurrent, Ecological, and Predictive", *Validity: Criterion, Concurrent, Ecological, and Predictive*, Routledge, doi: 10.4324/9780367198459-REPRW156-1.
- Min, K., Lee, J.-W. and Lee, B. (2019), "Improving Reliability of Smart Contracts and DApps by Applying Property-based and Model-based Test Methods to Different Test Levels", *Journal of KIISE*, Korean Institute of Information Scientists and Engineers, Vol. 46 No. 8, pp. 763–773, doi: 10.5626/JOK.2019.46.8.763.
- Miraz, M.H. and Ali, M. (2018), "Applications of blockchain technology beyond cryptocurrency", *Annals of Emerging Technologies in Computing*, Vol. 2 No. 1, pp. 1–6, doi: 10.33166/AETiC.2018.01.001.
- Mittwede, S.K. (2012), "Research Paradigms and Their Use and Importance in Theological Inquiry and Education", <https://doi.org/10.1177/205699711201600104>, SAGE PublicationsSage UK: London, England, Vol. 16 No. 1, pp. 23–40, doi: 10.1177/205699711201600104.

- Mohammed, S., Fiaidhi, J., Ramos, C., Kim, T.H., Fang, W.C. and Abdelzaher, T. (2021), "Blockchain in eCommerce: A Special Issue of the ACM Transactions on Internet of Things", *ACM Transactions on Internet Technology*, Vol. 21 No. 1, pp. 1–5, doi: 10.1145/3445788.
- Mohanty, D. (2018a), "Basic Solidity Programming", *Ethereum for Architects and Developers*, Apress, Berkeley, CA, pp. 55–103, doi: 10.1007/978-1-4842-4075-5_3.
- Mohanty, D. (2018b), "Testing Strategy for Ethereum Dapps", *Ethereum for Architects and Developers*, Apress, Berkeley, CA, pp. 197–201, doi: 10.1007/978-1-4842-4075-5_8.
- Mohit, J. (2023), "Angular vs React vs Vue: Core Differences | BrowserStack", available at: <https://www.browserstack.com/guide/angular-vs-react-vs-vue> (accessed 4 December 2024).
- Möller, D.P.F. (2020), "Cybersecurity in Digital Transformation", Springer International Publishing, Cham, doi: 10.1007/978-3-030-60570-4.
- Monrat, A.A., Schelen, O. and Andersson, K. (2020), "Performance Evaluation of Permissioned Blockchain Platforms", *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering, CSDE 2020*, Institute of Electrical and Electronics Engineers Inc., doi: 10.1109/CSDE50874.2020.9411380.
- Monti, M. and Rasmussen, S. (2017), "RAIN: A Bio-Inspired Communication and Data Storage Infrastructure", *Artificial Life*, Vol. 23 No. 4, pp. 552–557, doi: 10.1162/ARTL_a_00247.
- Moosavi, N. and Taherdoost, H. (2023), "Blockchain Technology Application in Security: A Systematic Review", *Blockchains 2023, Vol. 1, Pages 58-72*, Multidisciplinary Digital Publishing Institute, Vol. 1 No. 2, pp. 58–72, doi: 10.3390/BLOCKCHAINS1020005.
- Mougayar, W. and Vitalik Buterin. (2016), "The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology | Wiley", Wiley, p. 208.
- Muthurajkumar, S. (2021), *Preserving Data Integrity with Optimal Authentication in Cloud Computing*, *JETIR2101144 Journal of Emerging Technologies and Innovative Research*, Vol. 8.
- Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*.
- Nishant, J. (2019), "This is How Digital Platforms are Rapidly Disrupting the Tour and Travel Industry", available at: <https://www.entrepreneur.com/article/332133> (accessed 17 October 2021).
- Nofer, M., Gomber, P., Hinz, O. and Schiereck, D. (2017), "Blockchain", *Business and Information Systems Engineering*, Vol. 59 No. 3, pp. 183–187, doi: 10.1007/s12599-017-0467-3.

- Oghene, A.O. (2023), "Data breach and privacy in the digital era", *BOHR International Journal of Computer Science*, Vol. 2 No. 1, pp. 29–45, doi: 10.54646/bijcs.2023.14.
- Omolara, A.E. and Jantan, A. (2019), "Modified honey encryption scheme for encoding natural language message", *International Journal of Electrical and Computer Engineering*, Institute of Advanced Engineering and Science, Vol. 9 No. 3, pp. 1871–1878, doi: 10.11591/IJECE.V9I3.PP1871-1878.
- Omolara, A.E., Jantan, A., Abiodun, O.I., Arshad, H. and Mohamed, N.A.E. (2019), "Fingereye: Improvising security and optimizing ATM transaction time based on iris-scan authentication", *International Journal of Electrical and Computer Engineering*, Institute of Advanced Engineering and Science, Vol. 9 No. 3, pp. 1879–1886, doi: 10.11591/IJECE.V9I3.PP1879-1886.
- Peffer, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S. (2007), "A design science research methodology for information systems research", *Journal of Management Information Systems*, Vol. 24 No. 3, pp. 45–77, doi: 10.2753/MIS0742-1222240302.
- Peng, L., Feng, W., Yan, Z., Li, Y., Zhou, X. and Shimizu, S. (2021), "Privacy preservation in permissionless blockchain: A survey", *Digital Communications and Networks*, Elsevier, Vol. 7 No. 3, pp. 295–307, doi: 10.1016/J.DCAN.2020.05.008.
- Piscini, E. and Kehoe, L. (2018), "Blockchain & Cyber Security . Let ' s Discuss For more information please contact :", *Deloitte*, p. 14.
- Pongnumkul, S., Siripanpornchana, C. and Thajchayapong, S. (2017), "Performance analysis of private blockchain platforms in varying workloads", *2017 26th International Conference on Computer Communications and Networks, ICCCN 2017*, No. December 2018, doi: 10.1109/ICCCN.2017.8038517.
- Pramulia, D. and Anggorojati, B. (2020), "Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask", *Proceedings - 2nd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2020*, Institute of Electrical and Electronics Engineers Inc., pp. 18–23, doi: 10.1109/ICIMCIS51567.2020.9354310.
- Prasuna K S, Sermakani. A. M and Paruvathavarthini M. (2020), *Data Sharing with Sensitive Information Hiding in Data Storage Using Cloud Computing*.
- Qadir Mir, S., Ahmad Mir, I. and Maqbool Beigh, B. (2018), *Investigating the Denial of Service Attack: A Major Threat to Internet and the Security of Information*, *JK Research Journal in Mathematics and Computer Sciences*.
- Qammar, A., Ding, J. and Ning, H. (2021), "Federated learning attack surface: taxonomy, cyber defences, challenges, and future directions", *Artificial Intelligence Review 2021 55:5*, Springer, Vol. 55 No. 5, pp. 3569–3606, doi: 10.1007/S10462-021-10098-W.

- Qammar, A., Karim, A., Ning, H. and Ding, J. (2023), “Securing federated learning with blockchain: a systematic literature review”, *Artificial Intelligence Review*, Springer Nature, Vol. 56 No. 5, pp. 3951–3985, doi: 10.1007/S10462-022-10271-9/TABLES/6.
- Quackenbush, C. (2017), “Airbnb, Niido Land \$200 Million Investment For Branded Apartments | Fortune”, available at: <https://fortune.com/2017/12/19/airbnb-niido-branded-apartments-investment/> (accessed 18 October 2021).
- Quasim, M.T., Khan, M.A., Algarni, F., Alharthy, A. and Alshmrani, G.M.M. (2020), “Blockchain Frameworks”, No. February, pp. 75–89, doi: 10.1007/978-3-030-38677-1_4.
- Quluzada, J. and Maharramli, S. (2019), *The Development of Blockchain Technology*, doi: 10.2760/901029.
- Raturi, G. (2020), “Blockchain Technology Ensuring Data Security & Immutability | by Gautam Raturi | Towards Data Science”, available at: <https://towardsdatascience.com/blockchain-technology-ensuring-data-security-immutability-7150d309352c> (accessed 12 May 2021).
- Reid, R.C. and Gilbert, A.H. (2010), “Using the Parkerian Hexad to introduce security in an information literacy class”, *Proceedings of the 2010 Information Security Curriculum Development Annual Conference, InfoSecCD’10*, pp. 45–47, doi: 10.1145/1940941.1940953.
- Reuver, M. de, Sørensen, C. and Basole, R.C. (2018), “The Digital Platform: A Research Agenda”, *https://doi.org/10.1057/S41265-016-0033-3*, SAGE PublicationsSage UK: London, England, Vol. 33 No. 2, pp. 124–135, doi: 10.1057/S41265-016-0033-3.
- Robert, J. (2021), “Best Travel Booking Platforms Online”, available at: <https://offersnreviews.com/best-travel-booking-platforms-online> (accessed 17 October 2021).
- Rohm, A.J., Kashyap, V., Brashear, T.G. and Milne, G.R. (2004), “The use of online marketplaces for competitive advantage: a Latin American perspective”, *Journal of Business & Industrial Marketing*, Emerald Group Publishing Limited, Vol. 19 No. 6, pp. 372–385, doi: 10.1108/08858620410556318.
- Roslan, S.N., Hamid, I.R.A. and Shamala, P. (2018), “E-Store Management Using Bell-LaPadula Access Control Security Model”, *JOIV: International Journal on Informatics Visualization*, Politeknik Negeri Padang, Vol. 2 No. 3–2, pp. 194–198, doi: 10.30630/JOIV.2.3-2.140.
- Rossi, M., Mueller-Bloch, C., Thatcher, J.B. and Beck, R. (2019), “Blockchain research in information systems: Current trends and an inclusive future research agenda”, *Journal of the Association for Information Systems*, Vol. 20 No. 9, pp. 1388–1403, doi: 10.17705/1jais.00571.
- SACBC. (2024), “SACBC – The Southern African Catholic Bishops’ Conference”, available at: <https://catholicdirectory.org.za/> (accessed 13 February 2024).

- Saleem, T., Janjua, M.U., Hassan, M., Ahmad, T., Tariq, F., Hafeez, K., Salal, M.A., *et al.* (2022), "ProofChain: An X.509-compatible blockchain-based PKI framework with decentralized trust", *Computer Networks*, Elsevier, Vol. 213, p. 109069, doi: 10.1016/J.COMNET.2022.109069.
- Samonas, S. and Coss, D. (2014), "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security".
- Schäffer, M., di Angelo, M. and Salzer, G. (2019), "Performance and Scalability of Private Ethereum Blockchains", *Lecture Notes in Business Information Processing*, Springer Verlag, Vol. 361, pp. 103–118, doi: 10.1007/978-3-030-30429-4_8/COVER.
- Schlesinger, M. (2020), "A Growing Digital Economy Means More Cybersecurity Challenges", available at: <https://www.forbes.com/sites/forbestechcouncil/2020/11/30/a-growing-digital-economy-means-more-cybersecurity-challenges/?sh=4fa02640470a> (accessed 11 October 2021).
- Seebacher, S. and Schüritz, R. (2017), "Blockchain technology as an enabler of service systems: A structured literature review", *Lecture Notes in Business Information Processing*, Vol. 279 No. April, pp. 12–23, doi: 10.1007/978-3-319-56925-3_2.
- Shankar, A., Shetty, R. and Nath, B. (2019), *A Review on Phishing Attacks*, *International Journal of Applied Engineering Research*, Vol. 14.
- Sharma, Dr.L.R., Bidari, S., Bidari, D., Neupane, S. and Sapkota, R. (2023), "Exploring the Mixed Methods Research Design: Types, Purposes, Strengths, Challenges, and Criticisms", *Global Academic Journal of Linguistics and Literature*, SASPR Edu International Pvt. Ltd, Vol. 5 No. 1, pp. 3–12, doi: 10.36348/gajll.2023.v05i01.002.
- Shashi, S., Yadav, S. and Mishra, A. (2020), "A Prototype for Data Integrity in Cloud Environment", *EAI Endorsed Transactions on Cloud Systems*, European Alliance for Innovation n.o., Vol. "6" No. 18, p. 166287, doi: 10.4108/EAI.7-9-2020.166287.
- Shore, M., Zeadally, S. and Keshariya, A. (2021), "Zero Trust: The What, How, Why, and When", *Computer*, IEEE Computer Society, Vol. 54 No. 11, pp. 26–35, doi: 10.1109/MC.2021.3090018.
- Shree, D., Kumar Singh, R., Paul, J., Hao, A. and Xu, S. (2021), "Digital platforms for business-to-business markets: A systematic review and future research agenda", *Journal of Business Research*, Elsevier Inc., Vol. 137 No. August, pp. 354–365, doi: 10.1016/j.jbusres.2021.08.031.
- Skowroński, R. and Brzeziński, J. (2022), "UI dApps Meet Decentralized Operating Systems", *Electronics (Switzerland)*, MDPI, Vol. 11 No. 19, pp. 1–33, doi: 10.3390/ELECTRONICS11193004/.

- Soraya, S., Binti, L. and Kamal, A. (2019), "RESEARCH PARADIGM AND THE PHILOSOPHICAL FOUNDATIONS OF A QUALITATIVE STUDY", *International Journal of Social Sciences*, Vol. 4 No. 3, pp. 1386–1394, doi: 10.20319/pijss.2019.43.13861394.
- Steinheimer, M., Trick, U., Fuhrmann, W., Ghita, B. and Frick, G. (2017), "M2M Application Service Provision: An Autonomous and Decentralised Approach", *Journal of Communications*, Engineering and Technology Publishing, pp. 489–499, doi: 10.12720/JCM.12.9.489-499.
- Szabo, N. (2018), "Smart Contracts : Building Blocks for Digital Markets".
- Taherdoost, H. (2022), "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview", *Electronics 2022*, Vol. 11, Page 2181, Multidisciplinary Digital Publishing Institute, Vol. 11 No. 14, p. 2181, doi: 10.3390/ELECTRONICS11142181.
- Tapscott, D. and Tapscott, A. (2018), "Blockchain revolution : how the technology behind bitcoin and other cryptocurrencies is changing the world", p. 358.
- Tasevski, P. (2019), *Password Attacks and Generation Strategies*.
- Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M. and Choo, K.K.R. (2020), "A systematic literature review of blockchain cyber security", *Digital Communications and Networks*, Elsevier Ltd, Vol. 6 No. 2, pp. 147–156, doi: 10.1016/j.dcan.2019.01.005.
- Tosh, D., Shetty, S., Foytik, P., Kamhoua, C. and Njilla, L. (2018), "CloudPoS: A Proof-of-Stake Consensus Design for Blockchain Integrated Cloud", *IEEE International Conference on Cloud Computing, CLOUD*, IEEE Computer Society, Vol. 2018-July, pp. 302–309, doi: 10.1109/CLOUD.2018.00045.
- Troup, E. (2017), "Platforms are increasingly key to cybersecurity - TM Forum Inform", available at: <https://inform.tmforum.org/features-and-analysis/2017/05/platforms-increasingly-key-cybersecurity/> (accessed 11 October 2021).
- Truong, D., Le, T.T., Senecal, S. and Rao, S.S. (2021), "Electronic Marketplace: A Distinct Platform for Business-to-Business (B-to-B) Procurement", [Http://Dx.Doi.Org/10.1080/1051712X.2012.638467](http://Dx.Doi.Org/10.1080/1051712X.2012.638467), Taylor & Francis Group, Vol. 19 No. 3, pp. 216–247, doi: 10.1080/1051712X.2012.638467.
- Underwood, S. (2016), "Blockchain beyond bitcoin", *Communications of the ACM*, Association for Computing Machinery (ACM), Vol. 59 No. 11, pp. 15–17, doi: 10.1145/2994581.
- Vaishnavi, V. and Kuechler, B. (2004), *DESIGN SCIENCE RESEARCH IN INFORMATION SYSTEMS*.
- Valecha, V., Rudek, K., Szczepanik, G. and Palus, L. (2021), *Smart Data Protection*.

- Vitale, G. (2023), "Research Methodology", *SIDREA Series in Accounting and Business Administration*, Springer, Cham, Vol. Part F205, pp. 47–69, doi: 10.1007/978-3-031-30988-5_3.
- Wang, D., Zhao, J. and Wang, Y. (2020), "A Survey on Privacy Protection of Blockchain: The Technology and Application", *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., Vol. 8, pp. 108766–108781, doi: 10.1109/ACCESS.2020.2994294.
- Wang, H., Wang, Y., Cao, Z., Li, Z. and Xiong, G. (2019), "An overview of blockchain security analysis", *Communications in Computer and Information Science*, Vol. 970, pp. 55–72, doi: 10.1007/978-981-13-6621-5_5.
- Warkentin, M. and Orgeron, C. (2020), "Using the security triad to assess blockchain technology in public sector applications", *International Journal of Information Management*, Pergamon, Vol. 52, p. 102090, doi: 10.1016/J.IJINFOMGT.2020.102090.
- Wen, H., Fang, J., Wu, J. and Zheng, Z. (2021), "Transaction-based hidden strategies against general phishing detection framework on ethereum", *Proceedings - IEEE International Symposium on Circuits and Systems*, Institute of Electrical and Electronics Engineers Inc., Vol. 2021-May, doi: 10.1109/ISCAS51556.2021.9401091.
- Wooi Keong, Y. and Md Husin, M. (2021), "Understanding Research Paradigms: A Scientific Guide", doi: 10.47750/cibg.2021.27.02.588.
- Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., et al. (2022), "Cybersecurity, Data Privacy and Blockchain: A Review", *SN Computer Science 2022 3:2*, Springer, Vol. 3 No. 2, pp. 1–12, doi: 10.1007/S42979-022-01020-4.
- Yadav, V.S. and Singh, A.R. (2019), "A systematic literature review of blockchain technology in agriculture", *Proceedings of the International Conference on Industrial Engineering and Operations Management*, No. July, pp. 973–981.
- Yang, X., Yi, X., Nepal, S., Kelarev, A. and Han, F. (2020), "Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities", *Future Generation Computer Systems*, Elsevier B.V., Vol. 112, pp. 859–874, doi: 10.1016/J.FUTURE.2020.06.051.
- Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang, H. (2018), "Blockchain challenges and opportunities: A survey", *International Journal of Web and Grid Services*, Inderscience Publishers, Vol. 14 No. 4, pp. 352–375, doi: 10.1504/IJWGS.2018.095647.
- Zutshi, A., Grilo, A. and Nodehi, T. (2021), "The value proposition of blockchain technologies and its impact on Digital Platforms", *Computers and Industrial Engineering*, Elsevier Ltd, Vol. 155 No. January, p. 107187, doi: 10.1016/j.cie.2021.107187.

Appendices

Appendix 1: Selection Questionnaire

Research Title: Application of blockchain technology for data security: Case study of Global Mission Services' digital platform

Dear Participants,

My name is Yves Bizumuremyi, a master's student in information technology at the Central University of Technology, Free State, Bloemfontein, South Africa. I am conducting a study investigating the viability of using Blockchain technology to create a framework for securing data for service-based digital platforms. To do so, I must create a digital platform for all missionaries to test the feasibility of my research. I am requesting that you participate in this research by completing this questionnaire. Your responses to the questionnaire will assist me in identifying various catholic missionary organisations in South Africa and Eswatini, allowing me to begin the preliminary stage of our research. It will take between 5 to 10 minutes to complete this questionnaire.

Kind regards,

Yves Bizumuremyi
Student number: 221001962
Department of Information Technology,
Central University of Technology, Free State
Email: yvesbiu@gmail.com

Supervisor:

Ntima Mabanza
nmabanza@cut.ac.za

Please fill in the relevant information or select the correct answer.

Section 1: Organisational information and geographical location

1. Please indicate the name of your mission or centre (this is **optional**, and you can leave it blank if you are uncomfortable providing this information)

2. What is your position in the organisation (Mission)?

3. Where is your centre located?

- a) Eswatini
- b) South Africa

4. In how many countries does your organisation (Mission) have a presence?

5. In which of the following Regions are the countries you indicated in question 3 above found? You can select more than one

- a) Within the Southern African Development Community (SADC) countries
- b) Africa
- c) All around the world
- d) Other (Specify): _____

Section 2: Operational Details

6. How long have you been operating?

- a) Less than one year
- b) 2 to 3 Years
- c) 3 to 5 Years
- d) 5 to 10 Years
- e) 10 to 15 Years
- f) 15 to 20 Years
- g) More than 20 Years

7. How many people do you employ?

- a) 0-10
- b) 11-20
- c) 21-50
- d) More than 50

8. What is your monthly revenue

- a) Less than R20k
- b) R20k – 50k
- c) R50k – 100k
- d) More than 100k

Section 3: Services offered

9. What kind of services do you provide, or what facilities do you possess?

- a) Bed only
- b) Restaurant
- c) Bed & Breakfast
- d) Workshop & retreat centre

10. What is the purpose of the visit for most of your guests?

- a) Leisure
- b) Business
- c) Religious
- d) Other (Please Specify)

Section 4: Website information

11. Do you have a website?

- a) Yes
- b) No

If 'yes', please provide the URL.

Thank you for taking time to respond to this questionnaire.

Appendix 2: Online Security and Website Usage Questionnaire

Application of blockchain technology for data security: Case study of Global Mission Services' digital platform

Dear Participants,

I appreciate you for taking the time to respond to my preliminary questionnaire. The current questionnaire is the continuation of the previous one. Please accept my invitation to participate in this study by responding to it. This questionnaire seeks to understand your thoughts on the security of modern technology. It will take between 5 to 10 minutes to complete. Thank you for taking the time to respond to this questionnaire. Your response is significant and will assist me in improving online data security. I appreciate your participation and hope to use this information in my study to provide you with a better online security experience.

Kind regards,

Yves Bizumuremyi
Student number: 221001962
Department of Information Technology,
Central University of Technology, Free State
Email: yvesbiu@gmail.com

Supervisor:
Ntima Mabanza
nmabanza@cut.ac.za

Section 1: Purpose of Website and Electronic Equipment Usage

Please select the correct answer.

12. For what purpose do you use the website?

- a) Online Booking
- b) Advertising
- c) All the above

13. What kind of electronic equipment do you primarily use to access the website?

- a) Cell phone
- b) Computer
- c) Tablet
- d) Other (Specify)

Section 2: Perception of Online Security

Please indicate and rate your opinion on a scale of 1-5. Place a circle around the appropriate number, where:

1 = “Strongly Disagree”, 2 = “Disagree”, 3 = “Not Sure”, 4 = “Agree”, 5 = “Strongly Agree”

I. Confidentiality						
No	I.1. Authentication	SD	D	NS	A	SA
14.	I struggle with remembering my password to log in.	1	2	3	4	5
15.	I worry about the security of my password online.	1	2	3	4	5
16.	I use less secure passwords because more complicated passwords are harder to remember.	1	2	3	4	5
	I.2 Authorisation	SD	D	NS	A	SA
17.	It is essential to protect my sensitive information online.	1	2	3	4	5
18.	I have experienced the loss of my sensitive personal information online because of a digital attack.	1	2	3	4	5
19.	I have experienced someone having unauthorised access to my website or social media account.	1	2	3	4	5
	I.3 Accountability	SD	D	NS	A	SA
20.	I know the protection of sensitive information policy	1	2	3	4	5

21.	I know how website and social media owners use my data	1	2	3	4	5
22.	I care about how the website and social media owners use my personal information.	1	2	3	4	5
23.	I feel comfortable disclosing my personal information on the internet.	1	2	3	4	5
	II. Integrity (preventing improper information alteration or destruction and ensuring the authenticity and non-repudiation of information)	SD D NS A SA				
24.	I feel secure conducting business online.	1	2	3	4	5
25.	I consider security aspects when deciding to conduct business online.	1	2	3	4	5
26.	I know how to navigate the digital platform setting	1	2	3	4	5
27.	I know how to set available security options on the digital platform	1	2	3	4	5
28.	My personal information has once been compromised online.	1	2	3	4	5
	III. Availability (Information accessibility online)	SD D NS A SA				
29.	My website or online platform has been hacked before.	1	2	3	4	5
30.	I have been denied access to my website or my social media account.	1	2	3	4	5
31.	I have been redirected to a different website unknowingly.	1	2	3	4	5

Thank you for taking the time to respond to this questionnaire.

Appendix 3: Consent Form

Consent to participate in developing global mission's Services digital platform.

I, the undersigned (Mr. /Mrs. /Ms.) do hereby voluntarily agree to participate in the above-mentioned research study conducted by Mr Yves Ndayisenga Bizumuremyi, a master's student from the Department of Information Technology at the Central University of Technology, Free State.

The following are the conditions for my participation in this study:

- My participation in this study is voluntary.
- I have the right to leave this study at any time.
- I understand that the digital platform is being tested, not my capabilities.
- I will not be compensated for participating in this study.
- All the information I will provide during this study will be used only for research purposes.
- All my personal information will remain confidential, and no information identifying me will be published.
- I will respond to all the study questions as honestly as possible.

I have carefully studied the above and understand and accept this agreement.

Signature of participant:

☐

Name (Please Print):

☐

Date:

☐

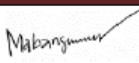
Signature of Witness:

Name (Please Print):

Date:

Appendix 4: Ethical Clearance

APPLICATION FORM FOR ETHICAL CLEARANCE: FEBIT

SIGNATURE (Main supervisor)	
SIGNATURE (Co-supervisor)	
DATE	15 March 2023

FOR OFFICIAL USE

APPROVAL OF FEBIT ETHICAL COMMITTEE (FRIC)

Please tick relevant decision and provide conditions/reasons where applicable		
Decision		Please tick relevant option
1.	Application approved	☒
2.	Ethical clearance number FRIC: 2023-03(1)	
3.	Application approved subject to certain conditions. <i>Specify conditions below</i>	
4.	Application not approved. <i>Provide reasons for non-approval below</i>	
SIGNATURE: Chairperson: Ethics committee 		
DATE 31/03/2023		

Cc Dean: FEBIT

Appendix 5: Graphs

A. Organisational information and geographical location

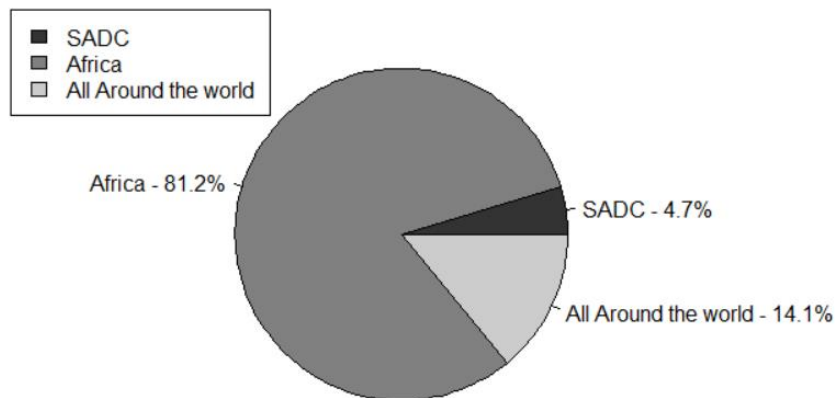


Figure 0.1. Centre's geographical location

B. Operational details

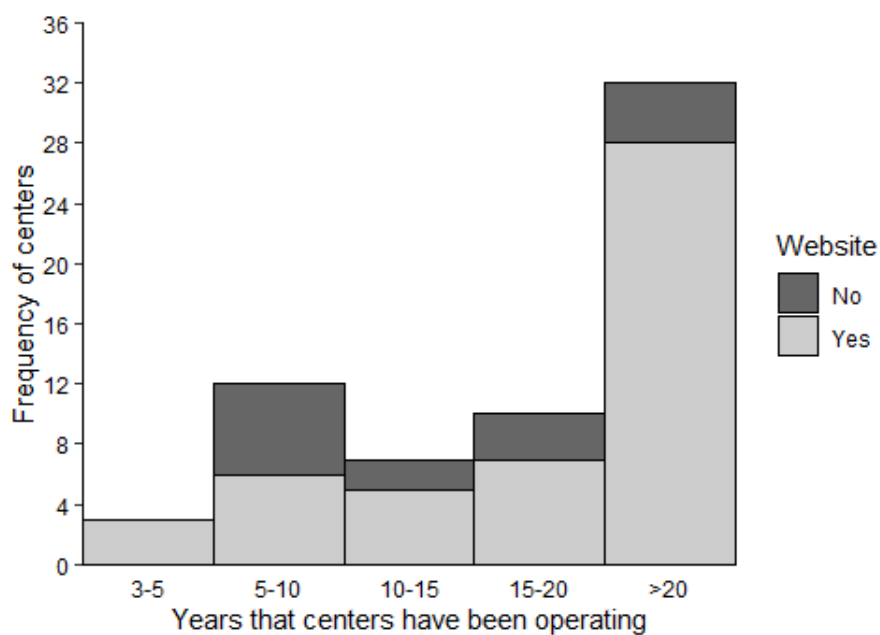


Figure 0.2. Frequency of centres with a functional website and the number of years they have been operating

C. Website information

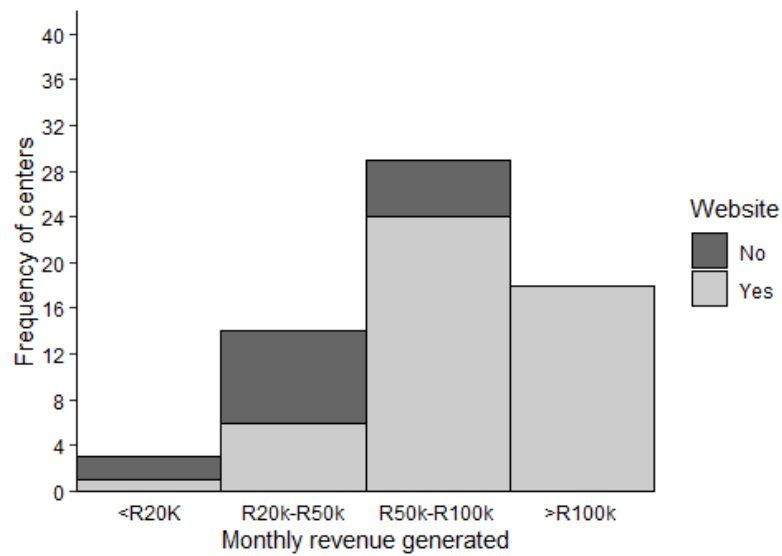


Figure 0.3. The number of centres and the generated monthly revenue

D. Website usage results

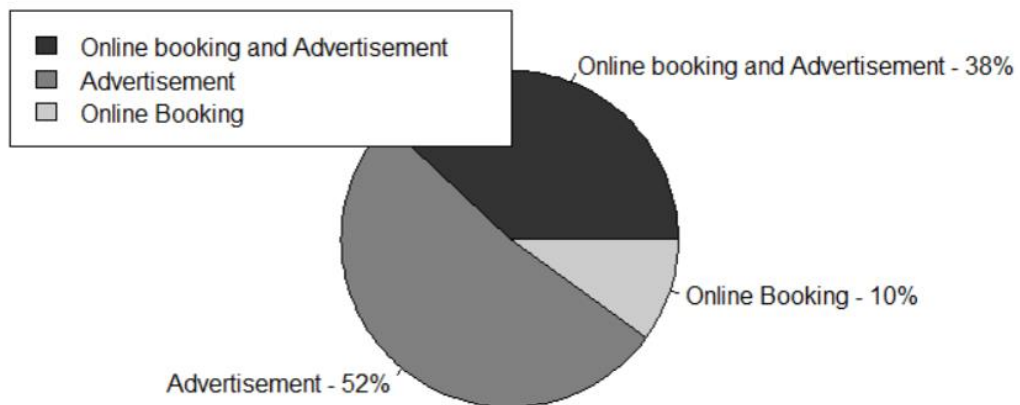
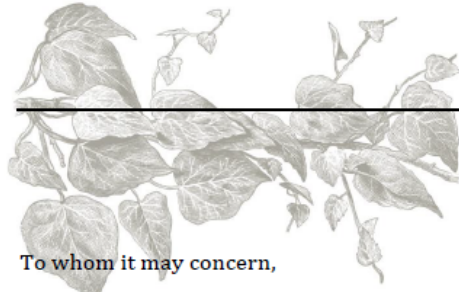


Figure 0.4. Website usage purpose

Appendix 6: Confirmation of Proofreading



Confirmation of Proofreading

30 August 2024

To whom it may concern,

CONFIRMATION OF PROOFREADING

In relation to the master's dissertation of Yves Ndayisenga Bizumuremyi (221001962), entitled:

APPLICATION OF BLOCKCHAIN TECHNOLOGY FOR DATA SECURITY: CASE STUDY OF GLOBAL MISSION SERVICES' DIGITAL PLATFORM

To be submitted in fulfilment of the degree Master of Information Technology at the Central University of Technology, Free State, I, in my capacity as Language Practitioner, confirm that the abovementioned document has been proofread, with specific focus on the following:

- Language use and spelling (UK English)
- Coherence and linguistic flow
- Consistency of terminology

In relation to the above, Track Changes were used in MS Word to indicate changes, and comments were provided where necessary. Please note that changes are made solely at the client's discretion and remain their own responsibility. Any comments provided are purely suggestions and reflect the best efforts and opinions of the Editor and not necessarily subject-specific expertise. It remains the responsibility of the client to confirm the content of their final submission.

For any questions, please feel free to contact me at guillaume.annam@gmail.com during normal business hours.

Kind regards,



A.M. Guillaume

LANGUAGE PRACTITIONER

Appendix 7: Smart Contracts Source code

Accommodation smart contract

```

Accommodation.sol X
src > contracts > Accommodation.sol
1  pragma solidity ^0.5.0;
2
3  contract Accommodation {
4      uint center_id;
5      string public name;
6      string public image;
7      uint public accitemCount = 0;
8      mapping(uint => Accitem) public accitems;
9
10     struct Accitem {
11         uint id;
12         uint center_id;
13         string name;
14         string image;
15         uint price;
16         uint room_num;
17         uint bed_num;
18         string description;
19         address payable owner;
20         bool isBooked;
21     }
22
23     event AccitemCreated(
24         uint id,
25         uint center_id,
26         string name,
27         string image,
28         uint price,
29         uint room_num,
30         uint bed_num,
31         string description,
32         address payable owner,
33         bool isBooked
34     );
35
36     constructor() public {
37
38     }
39
40     function createAccitem(
41         uint _center_id,
42         string memory _name,
43         string memory _image,
44         uint _price,
45         uint _room_num,
46         uint _bed_num,
47         string memory _description
48     ) public {
49         // Require a valid name
50         require(bytes(_name).length > 0);
51         //Validate Image
52         require(bytes(_image).length > 0);
53         // Require a valid description
54         require(bytes(_description).length > 0);
55         // Require a valid number of rooms
56         require(_room_num > 0);
57         // Require a valid number of beds
58         require(_bed_num > 0);
59         // Require a valid price
60         require(_price > 0);
61         // Increment product count
62         accitemCount++;
63         // Create the product
64         accitems[accitemCount] = Accitem(
65             accitemCount,
66             _center_id,
67             _name,

```

Conference smart contract

```
Conference.sol X
src > contracts > Conference.sol
1  pragma solidity ^0.5.0;
2
3  contract Conference {
4      uint center_id;
5      string public name;
6      uint public hallCount = 0;
7      mapping(uint => Hall) public halls;
8
9      struct Hall {
10         uint id;
11         uint center_id;
12         string name;
13         uint price;
14         uint capacity;
15         string description;
16         address payable owner;
17         bool isBooked;
18     }
19
20     event HallCreated(
21         uint id,
22         uint center_id,
23         string name,
24         uint price,
25         uint capacity,
26         string description,
27         address payable owner,
28         bool isBooked
29     );
30
31     constructor() public {}
32
33     function createHall(
34         uint _center_id,
35         string memory _name,
36         uint _price,
37         uint _capacity,
38         string memory _description
39     ) public {
40         // Require a valid name
41         require(bytes(_name).length > 0);
42         // Require a valid name
43         require(bytes(_description).length > 0);
44         // Require a valid capacity
45         require(_capacity > 0);
46         // Require a valid price
47         require(_price > 0);
48         // Increment product count
49         hallCount++;
50         // Create the product
51         halls[hallCount] = Hall(
52             hallCount,
53             _center_id,
54             _name,
55             _price,
56             _capacity,
57             _description,
58             msg.sender,
59             false
60         );
61         // Trigger an event
62         emit HallCreated(
63             hallCount,
64             _center_id,
65             _name,
66             _price,
67             _capacity,
```