Technological, Organisational, and Environmental Factors Affecting the Adoption of Blockchain-based Distributed Identity Management in Organisations

A dissertation submitted to the

Department of Information Systems

University of Cape Town

By

Sarah Mulombo Mulaji

(MLJSAR001)

Under the supervision of

Dr Sumarie Roodt

In partial fulfilment of the requirements for the Master of Commerce in

Information Systems degree

University of Cape Town

The copyright of this thesis vests in the author. No quotation from it or information derived from it is to be published without full acknowledgement of the source. The thesis is to be used for private study or non-commercial research purposes only.

Published by the University of Cape Town (UCT) in terms of the non-exclusive license granted to UCT by the author.

University of Cape Town

PLAGIARISM DECLARATION

I know that plagiarism is wrong. Plagiarism is to use another’s work and pretend that it is one's own.

I acknowledge that copying someone else’s work or essay, or part of it, to pretend it is one’s own is wrong.

This dissertation has been submitted to Turnitin and I confirm that my supervisor has seen my report and any concerns revealed by such have been resolved with my supervisor.

I certify that I have received Ethics approval from the Commerce Ethics Committee.

This work has not been previously submitted in whole, or in part, for the award of any degree in this or any other university. It is my own work. Each significant contribution to, and quotation in, this dissertation from the work, or works of other people has been attributed, and has been cited and referenced.

I have used the APA 7th edition for citation and referencing.

I have not allowed, and will not allow anyone, to copy my work to pass it off as theirs.

19 May 2022

Signed by candidate

Sarah Mulombo Mulaji.
MLJSAR001

ABSTRACT

Background: Blockchain is a disruptive technology with the potential to innovate businesses. Ignoring or resisting it might result in a competitive disadvantage for organisations. Apart from its original financial application of cryptocurrency, other applications are emerging, the most common being supply chain management and e-voting systems. However, there is less focus on information and cybersecurity applications, especially from the enterprise perspective. This research addresses this knowledge gap, focussing on its application of distributed identity management in organisations.

Objectives: The main objective is to investigate technological, organisational, and environmental (TOE) factors affecting the adoption of blockchain-based distributed identity management (BDIDM) in organisations to determine the most critical factors. Secondary objectives include determining whether the blockchain type affects BDIDM adoption and whether the TOE-BDIDM model measuring the phenomenon is effective and appropriate. But given the relative newness of blockchain, the initial goal consists of intensively exploring the topic to understand the practicality of adopting BDIDM in organisations and establishing whether claims made around it are factual than just due to the blockchain hype.

Methodology: The study uses meta-synthesis to explore the topic, summarising 69 papers selected qualitatively from reputed academic sources. The study then surveys 111 information and cybersecurity practitioners selected randomly in South African organisations to investigate the TOE factors affecting BDIDM adoption. To do so, it utilises an online questionnaire rooted in an adapted TOE model called TOE-BDIDM as a data collection instrument. The analysis of this primary data is purely quantitative and includes (i) Structural Equation Modelling (SEM) of the measurement model, i.e. confirmatory factor analysis (CFA); (ii) binary logistics regression analysis; and (iii) Chi-Square tests

Results: Meta-synthesis revealed theoretical grounds underlying claims made around the topic while spotting diverging views about BDIDM practicality for the enterprise context. It also identifies the TOE theory as more suitable to explain the phenomenon. Binary logistics regression modelling reveals that TOE factors do affect BDIDM adoption in organisations, either positively or negatively. The factors predict BDIDM adopters and non-adopters, with Technology Characteristics being the most critical factor and the most that could predict BDIDM non-adopters. Organisation Readiness was the second critical factor, the most that could predict BDIDM adopters. Overall, TOE-BDIDM effectively predicted 92.5% of adopters and 45.2% of non-adopters. CFA indicates that TOE-BDIDM appropriateness for investigating the phenomenon is relatively fair. The Chi-Square tests reveal a significant association between Blockchain Type and BDIDM adoption.

Implications: The discussion highlights various implications of the above findings, including the plausibility of the impartiality of typical privacy-preserving BDIDM models like the Self-sovereign identity: The majority of respondents preferred private permissioned blockchain, which tends to be centralised, more intermediated, and less privacy-preserving. The rest implications relate to the disruptiveness nature of BDIDM and the BDIDM adoption being more driven by technological than organisational or environmental factors. The study ends by reflecting on the research process and providing fundamental limitations and recommendations for future research.

RESEARCH OUTPUTS

Part of this dissertation is a published journal article, Mulaji & Roodt (2021), and a prospective journal article, Mulaji & Roodt (n.d), that is still under review at the time of writing. The following are the details of the two articles:

Mulaji, S.M. & Roodt, S. (2021). The Practicality of Blockchain-Based Distributed Identity Management in Organisations: A Meta-synthesis. *Security and Communication Networks*, vol. 2021, Article ID 9910078, 19 pages. https://doi.org/10.1155/2021/9910078

Mulaji, S.M. & Roodt, S. (n.d). Factors Affecting the Adopting Blockchain-based Distributed Identity Management in Organizations: A Survey of Information and Cybersecurity Practitioners in South Africa. [**Submitted to** the Special issue "Blockchain Technologies" of] *Sustainability 2022*.

ACKNOWLEDGEMENT

I am very grateful to God for life and grace to impact the world through research.

I appreciate sincerely my family; I would not have made it this far without their love and unwavering support.

My profound gratitude and thanks go to my supervisor Dr Sumarie Roodt, for their guidance, support, and constructive criticisms throughout the study; and for believing in me since the beginning.

I wish to acknowledge Professor Michael Kyobe, Wallace Chigona, and Irwin Brown for being incredible teachers, equipping me with the necessary knowledge and skills to undertake this research.

I also acknowledge Ms Zainab Ruhwanya for their helpful comments at one stage of this research. I thank all staff members and students of the Information System Department, University of Cape Town, for their contribution and encouragement in various ways.

A heartfelt thanks to all who contributed directly or indirectly in affording me an opportunity to further my studies and complete this degree in difficult times.

DEDICATION

I dedicate this dissertation to the memory of my late father, Sylvain Mulaja Diakabamba.

“Disruptive innovation can hurt, if you are not the one doing the disruption”.

—Clayton Christensen

Harvard Business School

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

1.1.Background

Identity management (IDM) is the first security barrier of a digital system that consists of two fundamental InfoSec principles: identification and authentication. Identification labels each user with an identifier, while authentication allows them to prove they are who they claim to be as a precondition to access the system. Identification and authentication are critical security measures because access to the system should only be granted to legitimate users. Hence, IDM mitigates security breaches. (Whitman & Mattord, 2018)

However, IDM faces many challenges that need to be addressed. Nearly every authentication method (such as passwords, biometrics, tokens, etc.) has known vulnerabilities and can be compromised (Whitman & Mattord, 2018). When users' credentials are compromised, the security of every system relying on them to authorise access is breached too (Alexander, 2020). Despite using multi-factor authentication to set up "strong authentication and identity verification" (ISO/IEC, 2014, p. 24), organisations still face data breaches. A growing tendency suggests this might be linked to the centralized architecture used in today's IDM systems (Liu et al., 2019).

Centralised IDM embeds a critical vulnerability of single point of failure (SPOF) (Shetty et al., 2019) because they use a central server to store the users' credentials and related identity data. When the server is compromised, users credentials related data is exposed, compromising both security and users' privacy (Maesa & Mori, 2020). Concerning privacy, Breuer et al. (2015) complement that managers face a dilemma of knowing "as much as possible about their (potential) customers" (p. 22) as part of the customer diligence rule. Yet, they need to preserve users' privacy in compliance with government regulations, such as the Protection of Personal Information Act (POPIA) in South Africa.

Meanwhile, the Internet growth has resulted in users with dozens of accounts with online services they subscribe to, forcing many to adopt insecure behaviour like reusing the same credentials with different services (Shehu et al., 2019). Others have been using weak credentials, so they are easier to remember, making it easier for imposters to guess them (Alexander, 2020). Moreover, "secure and reliable management of identities" is proven "the greatest challenges facing cloud computing today" (Bendiab et al., 2018, p. 724). Internet of thing (IoT) has rendered IDM even more complex due to the tremendous number of interconnected smart devices that interact with computers and humans today. Since “the security of these devices has not always been a primary concern” of their vendors, IoT increases the possible security breaches (Whitman & Mattord, 2018, p. 101).

That is why innovative IDM systems have been emerging, including blockchain-based distributed identity management (BDIDM). Despite blockchain’s immaturity as a technology (Demir et al., 2020), the literature suggests that BDIDM could help address some of the above IDM challenges (Shetty et al., 2019). Due to its distributed, decentralised, and disintermediated features, BDIDM has “arguably no single point of failure vulnerability” (Kshetri, 2017, p. 1028). BDIDM systems like Self-Sovereign identity (SSI) are claimed to be privacy-preserving (Maesa & Mori, 2020), eliminating the need for multiple accounts by enabling identity interoperability among different online services (Bernabe et al., 2019). SSI might also facilitate ‘secure cloud’ and ‘secure IoT’ (Charanya & Aramudhan, 2016; Ma, 2015).

Therefore, organisations might consider adopting BDIDM to mitigate IDM challenges and avoid potential competitive disadvantages (Shetty et al., 2019). Meanwhile, Baker (2012) suggests that elements of technology, organisation, and environment constitute a full context of an enterprise. They argue that these elements have been shown to impact, by constraining or promoting, how an organisation “identifies the need, searches, and adopts new technologies” (p. 232).

1.2.Problem statement

Identity management, that is identification and authentication of users online, is the first security barrier of a digital system that ensures access is only granted to authorised users. However, Identity management faces many challenges, including (i) vulnerabilities in authentication methods, (ii) vulnerabilities in system architecture, (iii) imbalance between security and privacy, (iv) credential reuse and weak credential; and (v) the pressure to achieve ‘secure cloud’ and ‘secure IoT. Despite blockchain immaturity, it is suggested that BDIDM could help to address some of these challenges. Hence, organisations might consider adopting BDIDM. Technological, organisational, and environmental factors might explain how the firm context impacts the adoption of such innovation in organisations.

1.3. Research questions

Primary research question:

- How do technological, organisational, and environmental factors impact BDIDM adoption in organisations, and what is the most critical factor/s?

Secondary research questions:

- How does the blockchain implementation type impact BDIDM adoption in organisations?
- What is the extent of the effectiveness of the TOE model in predicting BDIDM adopters and non-adopters?
- What is the extent of the appropriateness of the TOE theory to the context of BDIDM adoption in organisations?

1.4. Research objectives

The purpose of this research was both descriptive and explanatory but not casual.

Primarily, the research sought to explain how TOE factors impacted the decision to adopt BDIDM in organisations and determine which factor was the most critical. Since the study was not experimental, it was not necessarily interested in establishing what exactly caused the factors to impact that decision in such ways. It was all about determining (i) whether a relationship exists between TOE factors and BDIDM adoption, (ii) the nature and significance of the impact of every factor of the model on the adoption decision, and (iii) which was the most critical factor/s of all.

Secondarily, given the divergence around the practicality of BDIDM in organisations, the study was interested in determining whether the item (iv) blockchain implementation types had any individual significance on the decision to adopt BDIDM in organisations. Moreover, the research sought to assess the TOE's effectiveness and appropriateness in the context of BDIDM adoption in an organisation. Effectiveness was about determining (v) the curacy rate of the factors altogether in predicting adopters and non-adopters of BDIDM. Appropriateness was about (vi) assessing the extent of the model fitness to the data and its suitability for investigating the phenomenon, but not limited to these.

1.5.Thesis statement and research assumptions

This dissertation argues that TOE factors significantly impact the adoption of BDIDM in organisations positively or negatively. It also argues that some factors are more critical to the adoption than others since the practicality of BDIDM adoption in organisations is questionable. Additionally, the dissertation argues that the TOE model is effective and appropriate for investigating the phenomenon.

The dissertation bases this statement on the following assumptions. Next to each assumption is described the type of evidence provided throughout the dissertation to support it:

- Claims made about Blockchain, including its potential to address IDM challenges in organisations, are factual than just a result of hype. The literature review documented some theoretical evidence underlaying the claim to understand truthfulness.
- BDIDM is very disruptive for organisations compared to traditional IDM systems. The literature review gave a compressive background to understand contrasts between BDIDM and traditional IDM.
- BDIDM adoption and might be impractical from the enterprise perspective due to its disruption level. The literature review sported various perspectives around the concept of ‘BDIDM for enterprise’.
- There is a relationship between the TOE factors and BDIDM adoption in organisations. The empirical study provided evidence through statistical hypothesis testing.
- In the context of BDIDM, some TOE factors are more statistically significant than others. The empirical study provided evidence through statistical hypothesis testing.
- The TOE model could accurately predict adopters and non-adopters of BDIDM. The empirical evidence in terms of the TOE predictive accuracy rate.
- The adoption of BDIDM in organisations can be explained using the TOE theory. Sported in the literature review, then investigated empirically.
- InfoSec practitioners are knowledgeable enough to decide whether BDIDM is practical enough to be adopted by their respective organisations, hence were target respondents. Spotted in the literature and empirically proved by relatively acceptable reliability and validity of the data collected.

1.6.Research contribution

This research yielded some contributions to both the practice and the theory.

The practical contribution of this research principally consists of demystifying the concepts around the topic. The literature gave a comprehensive synthesis portraying a more pragmatic and enterprise perspective of BDIDM to assist potential organisations-adopters, particularly InfoSec practitioners deciding for adoption on behalf of their companies, in making an informed decision. The empirical evidence might attract further experiments to maximise the blockchain potential to solve this global issue of IDM challenges. The research can inspire other empirical studies on blockchain topics that are still lacking.

The theoretical contribution essentially comprised the operationalisation, testing, assessment, and reflection on the TOE theory in the context of BDIDM adoption in organisations. This enterprise-level adoption theory has not yet been given much attention compared to other competing adoption theories. The empirical evidence shows the extent of TOE explanatory and predictive capabilities in the context of BDIDM adoption. Another theoretical contribution consisted in documenting theoretical evidence underlying some of the claims made about blockchain and BDIDM, using one or a combination of random theories such as the CIA triad, TSF, SPOF, Zero Trust, etc.

1.7. Dissertation layout

This dissertation is structured into five chapters: (i) introduction, (ii) literature review, (iii) research design and methodology, (iv) analysis, finding and discussion, and (v) conclusion. The Introduction chapter outlined the study purpose, giving the research questions, objective, thesis statement, assumptions, and contributions. The literature review chapter explores the topic, focusing on how practical BDIDM was from the enterprise perspective to see if claims around it had any theoretical foundation. The research methodology and design chapter discusses the methodological framework followed in undertaking this research, from the research philosophy to techniques and procedures of data collection and analysis. The analysis, findings, and discussion chapter first report the results of the statistical analysis performed data, then discuss their implications considering the research objectives and assumptions, mirroring with the literature review perspectives. The conclusion chapter summarises the research findings, outlines the research limitations and provide recommendation for further research.

CHAPTER 2: LITERATURE REVIEW

2.1. Introduction

“Issues related to data integrity are most acute, as data tampering can have a huge impact on mission-critical services that depend upon reliable data” (Shetty et al., 2019, p. XIII). One of the fundamental steps in enforcing data integrity is safeguarding the digital system —i.e., networks, websites, databases, applications, etc.— using the data through effective identification and authentication management. In this way, only authorised people can access the system and potentially use the data. Yet, data breaches and their consequences are still occurring, making current IDM systems to some extend questionable (Maesa & Mori, 2020). For example, a Serianu report revealed that Africa has one of the highest cybercrimes and financial losses (Musuva-Kigen et al., 2016). The IBM 2019 Cost of a Data Breach Study reported an increase in the average cost of a data breach in South Africa, by12% from 2018 to 2019 (IBM-Security, 2019) and would increase with the impact of the COVID-19 pandemic.

Meanwhile, several claims are increasingly made about the potential of blockchain to provide a way forward in managing digital identities. Some studies claim that (i) “Blockchain solutions for cybersecurity could represent a paradigm shift in how data manipulation will be defended by creating a trusted system in a trustless environment” and that (ii)“Blockchain could address cybersecurity challenges such as Identity management” (Shetty et al., 2019, p. XIII). Others claim that (iii) Blockchain systems have “arguably no single point of failure vulnerability” (Kshetri, 2017, p. 1028) and that (iv) Blockchain identities are privacy-preserving and (v) ‘give back to users their power over their data’ (Kuperberg, 2019). Further claims suggest that (vi) centralized IDM systems are “subject to different problems and threats such as data breaches” (Bernabe et al., 2019, p. 164913), hence should (vii) evolve to possess distributed, disintermediated and secure capabilities” (Shetty et al., 2019). Therefore, it was worthwhile to explore blockchain as a use case for IDM in organisations.

This literature review explored how practical BDIDM was from the organisational perspective, providing a comprehensive background to understand the topic. The review included understanding whether claims about Blockchain concerning IDM, especially blockchain potential to address IDM challenges, are based on facts or just a result of hype. Because there is so much ambiguity around blockchain topics, “their true nature is often obscured by marketing and hype” (Kolb et al., 2020, p. 9:1).

The findings covered both the concept and theory aspects of the topic narratively. Concepts describe the topic by laying the basics about its two key components: identity management and blockchain technology, including their relationships (especially the implications of the organisational context). Theories made sense of the topic; on the one hand, by interpreting the underlying facts of the claims made, on the other hand by explaining the topic using a suitable enterprise-level adoption theory. The following section gives more details about the research methodology followed in conducting the review.

2.2. Review methodology

This explorative review followed a "qualitative meta-aggregation and meta-summary" research methodology called meta-synthesis that seeks to summarise and "distil information to draw conclusions" (Finfgeld-Connett, 2018, p. 10-11) while creating "refined meanings, exploratory theories and new concepts". It is rooted in an interpretive approach and aims to "rigorously synthesize qualitative research findings" to produce generalisable knowledge. (Walsh & Downe, 2005, p. 208-209)

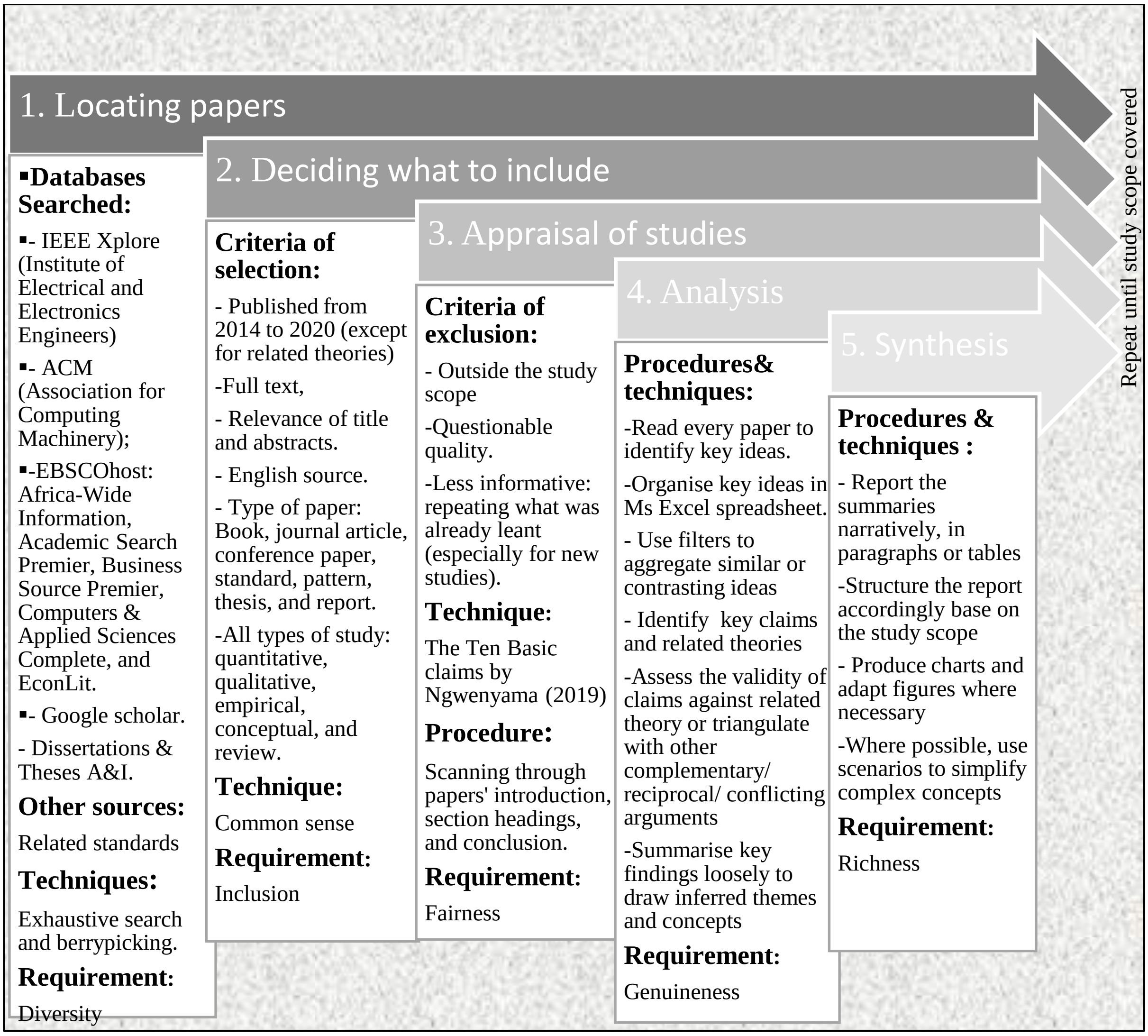
This review opted for a realist meta-synthesis by combining positive and interpretive approaches to overcome their respective limitations, including all types of studies: quantitative, qualitative, empirical, conceptual, and review. This realist meta-synthesis shared some similarities with a systematic review, predefining most of the rules followed during the review process (Oosterwyk et al., 2019). The main difference with a systematic review was that the review process was repeated several times to mature the review scope and satisfy the richness requirement of a qualitative study. Meta-analysis was not suitable because it is leaner, typically analyses findings across quantitative studies "to identify statistically significant results" (Finfgeld-Connett, 2018, p. 9-12), and tend to prioritise objectivity over richness (Walsh & Downe, 2005, p. 205). The predefined rules in this review were the review scope, data location (databases), search terms, selection criteria, exclusion criteria, and techniques & procedures of analysis and synthesis. The initial phase consisted of framing the review exercise, determining the scope of the review.

2.2.1. Framing the review exercise

Scoping meta-synthesis is still a debate, with some views advocating for "a narrower, more precise approach" and the others advocating for "a broader, more inclusive stance" (Walsh & Downe, 2005, p. 206). Since this review follows the realism philosophy, it considered a pragmatic approach by having the scope dictated by the themes that made up the topic and having it refined as needed to mature. After several refinements, the final scope retained four main themes (MT) that were further broken down into subthemes. Two main themes represent the fundamental concepts of the topic (MT1: ‘Identity Management’ and MT2: ‘Blockchain technology’), and two represent the interrelationships between them (MT3: ‘Enterprise Perspective of BDIDM and implementation proposals’, and MT4: ‘Related Theories’).

2.2.2. Phases of the Review Exercise

Figure 1 shows that the review exercise consisted of five phases repeated four times over a year as new papers were published: December 2019, March 2020, June 2020, and September 2020. The review did so to allow the maturity of the scope and accommodate the topic's relative newness at the time of writing. There was not much written on the topic at the beginning of the research process. The review ended when the topic was saturated: there was a repetition of what was already lent. The main requirements throughout the review process were to achieve *diversity* when locating papers, *inclusion* when deciding what to include, *fairness* when appraising studies, *genuineness* when analysing studies, and *richness & simplicity* when synthesising them.



▪Databases Searched:

▪- IEEE Xplore (Institute of Electrical and Electronics Engineers)

▪- ACM (Association for Computing Machinery);

▪-EBSCOhost: Africa-Wide Information, Academic Search Premier, Business Source Premier, Computers & Applied Sciences Complete, and EconLit.

▪- Google scholar.

- Dissertations & Theses A&I.

Other sources:

Related standards

Techniques:

Exhaustive search and berrypicking.

Requirement:

Diversity

Criteria of selection:

- Published from 2014 to 2020 (except for related theories)

-Full text,

- Relevance of title and abstracts.

- English source.

- Type of paper: Book, journal article, conference paper, standard, pattern, thesis, and report.

-All types of study: quantitative, qualitative, empirical, conceptual, and review.

Technique:

Common sense

Requirement:

Inclusion

Criteria of exclusion:

- Outside the study scope

-Questionable quality.

-Less informative: repeating what was already leant (especially for new studies).

Technique:

The Ten Basic claims by Ngwenyama (2019)

Procedure:

Scanning through papers' introduction, section headings, and conclusion.

Requirement:

Fairness

Procedures& techniques:

-Read every paper to identify key ideas.

-Organise key ideas in Ms Excel spreadsheet.

- Use filters to aggregate similar or contrasting ideas

- Identify key claims and related theories

-Assess the validity of claims against related theory or triangulate with other complementary/ reciprocal/ conflicting arguments

-Summarise key findings loosely to draw inferred themes and concepts

Requirement:

Genuineness

Procedures & techniques :

- Report the summaries narratively, in paragraphs or tables

-Structure the report accordingly base on the study scope

- Produce charts and adapt figures where necessary

-Where possible, use scenarios to simplify complex concepts

Requirement:

Richness

Figure 1. Summary of the activities of the five phases of the review exercise

Diversity in information sources was achieved by including unusual sources like reports, standards, and theses, often inaccessible from common databases. Therefore, in addition to those recommended for Information System studies (the five databases included in EBSCOhost), the review considered other databases to accommodate the technical side of the topic (IEEE and ACM) and generic ones like Google Scholar to boost diversity. Given the topic complexity and high variance rate of its concepts, the search terms were intentionally exhaustive to capture as much information as necessary to cover the scope of the review. As shown in Table 1 below, the search terms were derived from the four main themes and used one at a time in each predefined database. This data retrieval technique is also called "berrypicking of information" (Walsh & Downe, 2005, p. 205-207)

Table 1. List of search terms used to locate papers

Search terms
▪ (‘Identity Management’ OR ‘ÍDM’ OR ‘Identity and Access Control’ OR ‘IAM’) AND (issues OR challenges OR problems OR vulnerabilities OR implementation)
▪ (Blockchain OR distributed) AND (OR ‘Identity Management’ OR ‘Identity Authentication’ OR ‘Identity Proofing’ OR IDM)
▪ [Blockchain AND (identity OR ID)] AND (issues OR challenges OR weaknesses OR problem OR vulnerabilities)
▪ [(Permissioned OR Permissionless) AND Blockchain’] OR (‘Public Blockchain’ OR ‘Private Blockchain’ OR ‘Open blockchain’ OR ‘federated blockchain’)
▪ ‘Adoption of blockchain’ OR ‘blockchain adoption’ OR ‘Blockchain ID adoption’ OR ‘Distributed ID adoption’
▪ (‘Sigle point of failure’ AND ‘Identity management’ AND blockchain) OR [(central* OR distribut*) AND (architecture OR system)]

Inclusion was achieved by considering different types of papers, from books to unpublished theses, as well as considering studies with “different methodological approaches” since meta-synthesis embraces the challenging idea that “multiple approaches can be synthesized” (Walsh & Downe, 2005, p. 207). The remaining selection criteria were simply based on common sense.

Fairness of the results was ensured by assessing the quality of individual studies using the ten basic claims by Ngwenyama (2019) as part of the appraisal phase. Some studies often bypassed the appraisal stage, assuming that “the rigour of individual studies is less important than the attempt to be as inclusive as possible” (Walsh & Downe, 2005, p. 208). After all, the review adopted a centric approach that values both studies' inclusion and result’s fairness. In addition, the review assessed the validity of the claims made about the topic using related theories.

Originality of the findings was ensured by trying to preserve the original meaning of the text of individual studies while resisting, as much as possible, “the temptation to force a fit in the interests of illustrating homogeneity”, since “the links between studies may be reciprocal, complementary or conflicting”. Originality also partially justified the intense use of direct quotes. The selected studies were seriously reviewed to identify key ideas to aggregate and draw common themes and concepts. These were then “juxtaposed to identify homogeneity to note discordance and dissonance”. (Walsh & Downe, 2005, p. 208)

The richness of the account was achieved by opting for a narrative synthesis that “reflects the tension between contradictory or alternative explanations if reciprocal translations suggest a lack of congruence”. In this way, the synthesis provides a comprehensive background necessary to understand the links between concepts and the underlying debate around ‘enterprise BDIDM’. Eventually, the synthesis as a “whole is greater than the sum of the constituent parts”. To achieve simplicity while increasing comprehensibility, the review used illustrations, images, and scenarios to simplify complex concepts while using tables to summarise ideas involving a considerable amount of information (Walsh & Downe, 2005, p. 209)

2.2.3. Description of the sample

After completing several iterations of the five phases of the review exercise and saturating the topic, the final number of selected papers came to 69 (excluding those supporting the research methodology). Descriptive statistics (numbers, percentages, and charts) summarised the sample based on the type of studies and year of publication. The pie chart on the left-hand side of Figure 2 indicates the type of distribution of the sample in percentage, mainly of 32 conference papers (46.4%), 25 journal articles (36.2%), and six books (8.7%). The scatter chart on the right-hand side of Figure 2 indicates that approximately 84% (59) of the 69 papers were published between 2017 and 2020.

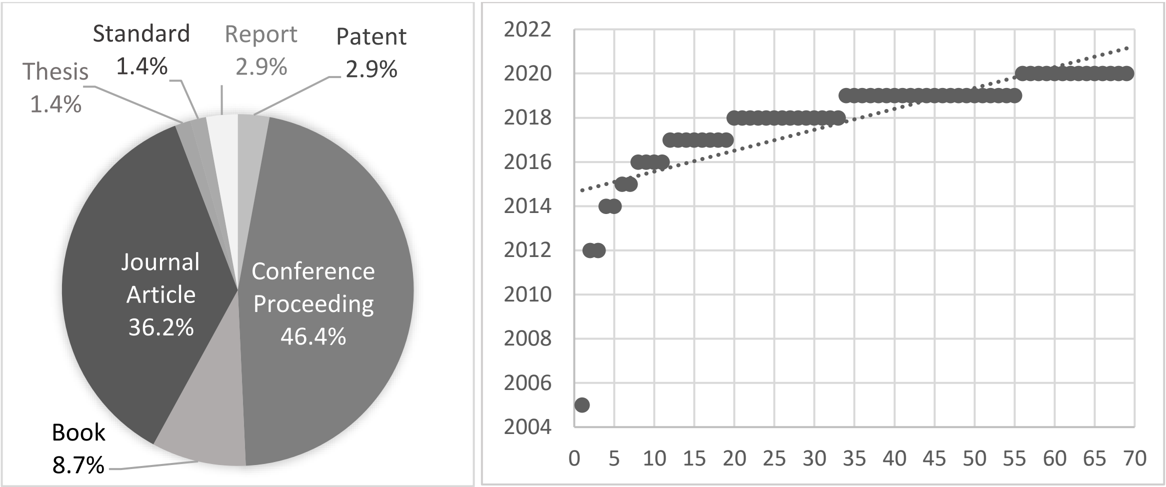
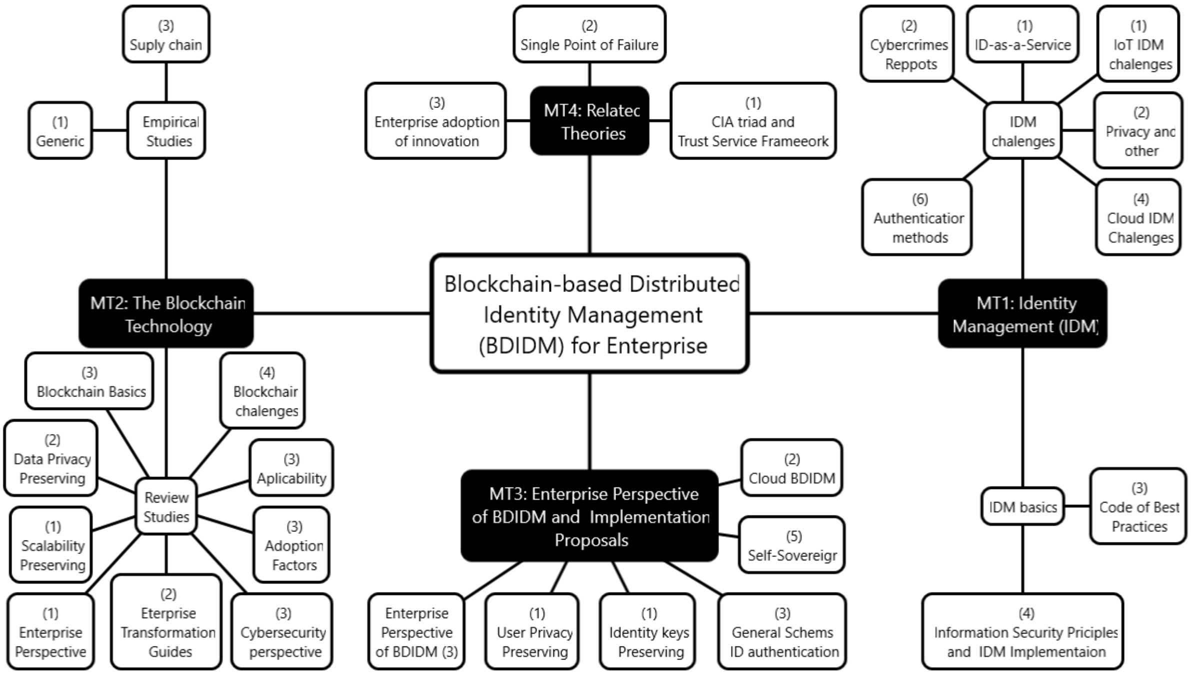


Figure 2. Description of the sample of papers: from the perspective of their type on the left-hand side and their year of publication on the right-hand side

Qualitative methods (thematical analysis) described the sample from the perspective of the review scope. Figure 3 shows how each selected paper relates to the review scope of the four main themes broken down into subthemes (and leaves-themes where possible). It also reports the number of papers retrieved per theme in bracket (n). In total, 26 papers felt under MT2: ‘The Blockchain technology’ (22 for ‘Review Studies’ and 4 for ‘Empirical studies’ subthemes), 23 papers under MT1: ‘Identity Management’ (16 for ‘IDM challenges’ and seven for ‘IDM Basics’ subthemes), 14 papers under MT3: ‘BDIDM Implementation Proposals and ‘Enterprise Perspective of BDIDM’, and six papers under MT4: ‘Related theories’.



(3) Suply chain
(1) Generic
Empirical Studies
(2) Single Point of Failure
(3) Enterprise adoption of innovation
MT4: Relatec Theories
(1) CIA triad and Trust Service Frameeork
(2) Cybercrimes Reppots
(1) ID-as-a-Service
(1) IoT IDM chalenges
IDM chalenges
(2) Privacy anc other
(6) Authenticatior methods
(4) Cloud IDM Chalenges
MT2: The Blockchain Technology
Blockchain-based Distributed Identity Management (BDIDM) for Enterprise
MT1: Identity Management (IDM)
(3) Blockchain Basics
(4) Blockchair chalenges
(2) Data Privacy Preserving
Review Studies
(3) Aplicability
(1) Scalability Preserving
(3) Adoptior Factors
(1) Enterprise Perspective
(2) Eterprise Transformation Guides
(3) Cybersecurity perspective
MT3: Enterprise Perspective of BDIDM and Implementatior Proposals
(2) Cloud BDIDM
(5) Self-Sovereigr
Enterprise Perspective of BDIDM (3)
(1) User Privacy Preserving
(1) Identity keys Preserving
(3) General Schems ID authentication
IDM basics
(3) Code of Best Practices
(4) Information Security Priciples and IDM Implementaion

Figure 3. Distribution of the selected papers according to their themes (with number of papers per them in bracket): the underlying structure of the review layout

2.3. Review layout

The review is narrative and structured in such a way to cover the main themes within the review scope, as shown in Figure 3. MT1 relates to IDM overview, IDM challenges that need to be addressed, and the evolution of IDM models to address IDM challenges. MT2 concerns Blockchain overview and blockchain promoting and constraining factors. MT3 discusses the practicality of BDIDM in organisations from different angles: concept, IDM model, blockchain implementation, and ability to address IDM challenges. MT4 assesses the validity of claims made about BDIDM throughout the review and explain factors that impact BDIDM adoption in organisations based on the TEO theory.

The following section of the review gives the fundamentals of IDM and highlight some critical IDM challenges needing to be addressed.

2.4. Identity management (IDM).

A *digital identity* is "a set of claims made by one digital subject about itself or another digital subject". A *digital subject* is the digital illustration of the defined individual, often referred to as an *entity*. A *claim* is an assertion of propriety about a subject. (Chakravarty & Deshpande, 2018, p. 1)

Technically, IDM consists of managing matters related to two fundamental InfoSec principles: *identification* and *authentication*. Identification and authentication are vital first steps in controlling access to a digital system, such as a corporate website, an application, a database, etc. On the one hand, identification proves that a user is who they claim to be. As illustrated below, this is imperative because access should only be granted to legitimate users (authorisation). On the other hand, authentication proves that a user acted on a system (accountability). Likewise, a user should not be able to deny what they have done (non-repudiation or non-denial). (Whitman & Mattord, 2018)

> Identification*: "I am a user of this system"* —here is my username: 'Alice';
> Authentication*: "I can prove I'm a user of this system"* —here is my password: 'All#125gef';
> Authorization*: "Here's what I can do with the system"* —I can view and edit 'Client_file.mdb';
> Accountability*: "You can track and monitor my use of the system"* —I cannot deny my actions. (Whitman & Mattord, 2018, p. 330)

An *IDM system* labels each entity with an identifier (usually in a human-friendly format, for instance, a meaningful string), providing a way for the entity to authenticate (often by proving knowledge of some private information, for example, a password, phone number PIN, biometrics, etc.) and stores its relevant identity information on a dedicated component (generally a server) (Maesa & Mori, 2020, p. 101).

2.5. The criticality of addressing IDM challenges in organisations

IDM is a fundamental security control that mitigates security breaches in organisations (Whitman & Mattord, 2018). However, IDM faces many challenges. The most common are vulnerabilities in authentication methods, vulnerabilities in system architecture, the imbalance between security and privacy, credential reuse and weak credential, and the pressure to achieve 'secure cloud' and 'secure IoT.

2.5.1. Vulnerabilities in authentication methods

Authentication is a principle of InfoSec that challenges the user to provide information that formally proves that they are known by the system and thus may officially log onto it. That information, also called user credentials, can take various forms, from passwords to biometrics, and can be implemented as an authentication method. (Whitman & Mattord, 2018)

Unfortunately, every authentication method has known vulnerabilities and can be compromised. Knowledge-based methods like passwords and PIN are vulnerable to guessing attacks like dictionary, rainbow table, bruteforce, etc. (Whitman & Mattord, 2018). Moreover, users may experience difficulties in matching their passwords to different accounts (Marky et al., 2018). Smart/magnetic cards can be lost or stolen. Hard biometrics, such as finger/palm prints and retina/iris scans, are relatively expensive to implement and invasive for users. In addition, their effectiveness depends on their false positives and false-negative rates (Kiran et al., 2018; Seitz et al., 2017). Soft biometrics methods such as signatures and typing patterns, as well as location-based methods such as the Global Positioning System (GPS) and Indore Positioning System (IPS), are only secondary to continuously verifying an authenticated user (Xiaofeng et al., 2019).

When users' credentials are compromised, the security of every system relying on them to authorise access is also breached. "Strong authentication requires a minimum of two authentication mechanisms drawn from two different authentication factors" (Whitman & Mattord, 2018). Therefore, codes of best practices in InfoSec, including the ISO/IEC and NIST, recommend the use of multifactor authentication (MFA) to establish "strong authentication and identity verification" (Hufstetler et al., 2017; ISO/IEC, 2014, p. 24). However, despite the use of MFA, organisations are still facing data breaches. The literature increasingly emphasises that another vital issue weakening IDM systems might be their traditional centralised architecture (Liu et al., 2019; Pranata & Nugroho, 2019).

2.5.2. Vulnerabilities in the IDM System Architecture

Centralised IDM embeds a critical vulnerability of single point of failure (SPOF), as they use a central server to store the identity data. When the server is compromised, identity data is exposed, and the server may no longer be available (Liu et al., 2019). SPOF is a well-known theory in security risk management. It suggests that when a system's overall functionality depends on a single node, there is a high risk for the whole system to collapse when that particular node fails. Some studies suggest that “multicopy redundancy technology"(Rauscher, 2005, p. 5) would mitigate the SPOF vulnerability and achieve reliability and resilience in digital systems (Clara, 2014; Feng et al., 2014). Redundancy involves having a duplicate copy of the database on every node, generally known as distribution (Dresher, 2017). That is why distributed systems, such as blockchains, have “arguably no single point of failure vulnerability” (Kshetri, 2017, p. 1028).

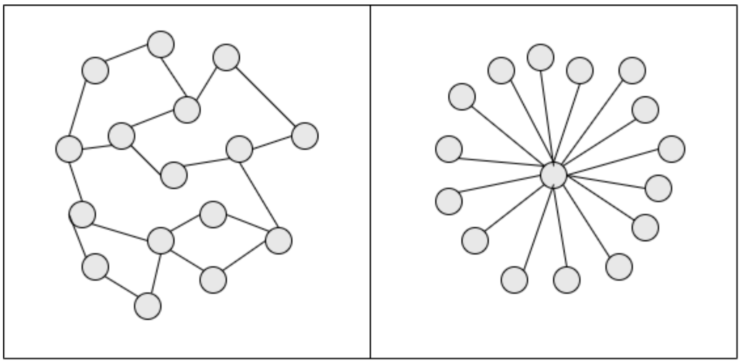


Figure 4. Distributed vs Centralised system architecture. Adapted from Dresher (2017)

In Figure 4 above, the left-hand side illustrates a distributed system where all nodes are equal and play the provider and consumer of services. If one node fails, the others can still take over. The right side illustrates a centralised system, such as the Client-Server, where the server provides services for clients to consume (Dresher, 2017). The failure of the server knocks the whole system down. (Liu et al., 2019). In a distributed system like blockchain, “more than 50%” of nodes must be compromised first to bring the entire system down, which is extremely difficult to achieve (Kshetri, 2017, p. 1027).

2.5.3. Balance between security and privacy

The ongoing data breaches in organisations indicate the need to ensure effective identity and access management systems (Karanja & Rosso, 2017). Sometimes, organisations undermine privacy since security managers face a dilemma about user identity data. On the one hand, organisations need to comply with their business strategy seeking for ‘user ownership’, which involves having direct contact with and getting much information as possible about their (potential) customers. On the other hand, security managers must protect users' privacy in compliance with government regulations like POPIA in South Africa. Users, of course, “want good services offered in convenient ways” yet are very “concerned about infringements to their privacy”.(Breuer et al., 2015, p. 22)

An example of a 'security and privacy conflicting' business requirement is the Know Your Customer regulation to verify clients' identities in the banking industry. This mitigates the risks posed by malicious customers and "is part of Anti Money Laundering initiatives " (Baars, 2016, p. 14). In this case, centralised IDM might be dangerous for customers' privacy as it endorses total control of customers' identity data to banks. Customers must trust banks not to exploit this data and "effectively protect it from external attacks" (Maesa & Mori, 2020, p. 105). This issue verifies the theory of 'the CIA triad' —an acronym for three fundamental objectives of InfoSec: *confidentiality*, *integrity*, and *availability*.

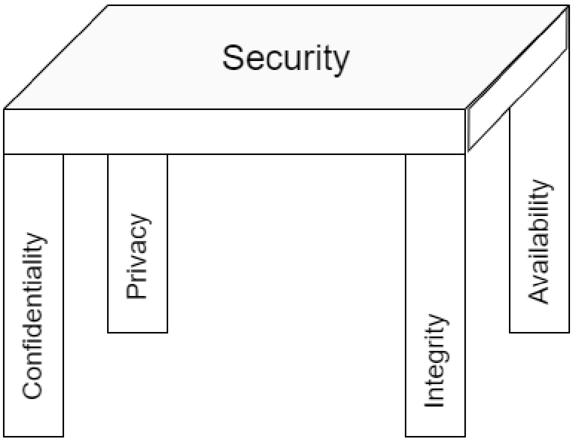


Figure 5. The CIA triad integrated with the Trust Service Framework

Whitman & Mattord indicate that the CIA triad "has been the standard for computer security in both industry and government since the mainframe development" (p. 11), apparently formally established by Donn Parker in 1998. This theory suggests that the security and reliability of a computer system depend on a balance between confidentiality, integrity, and availability. Confidentiality prevents unauthorized access to information, integrity prevents unauthorized modification of information, and availability ensures the information is always available to authorized users (Whitman & Mattord, 2018). However, another underlying requirement for a digital system is privacy. Privacy prevents unauthorized access to the personal data of employees, clients, partners, etc. Figure 5 illustrates a typical application of this extended CIA as the Trust Service Framework (TSF), developed by Romney et al. (2012) to guide the field of accounting information systems. Just as a four-legged table cannot balance if one leg is missing, the TSF suggests that security without privacy is problematic.

2.5.4. Credential reuse and weak credentials

The internet has grown significantly. As a result, numerous online services have forced users to have dozens of accounts with specific online services they subscribe to, causing the burden of matching every account with its credentials (Whitman & Mattord, 2018). Users have been reusing the same credentials on different services, creating redundant security data (Shehu et al., 2019). In this way, when one service is compromised, the security of all substantial services relying on the same credential to authorise access is also breached. Others use weak passwords, so they are easy to remember, making it easier for imposters to guess. Meanwhile, guessing engines known as bruteforce attacks are getting more sophisticated, using high computation power. In 2019, a hacker under the pseudonym 'Tinker' announced on Twitter that an open source password recovery tool could crack an 8-character Windows NTLM password hash in less than 2.5 hours.

2.5.5. 'Secure cloud' and 'secure IoT'

Initially, IDM systems used to identify a living individual in a digital system and involved authenticating them as a legitimate user of the system (Maesa & Mori, 2020). Today, IDM systems need to identify and authenticate not only individuals but also 'things' such as software, smartphone, robot, automobile, appliances, entertainment devices, etc. —hence the origin of the so-called IoT, an acronym for Internet of Things (Zhu & Badr, 2018). IoT has made IDM management even more complex than before due to the many interconnected smart devices interacting with computers and humans today. Since "the security of these devices has not always been a primary concern" of their vendors, IoT increases the possibility of security breaches (Whitman & Mattord, 2018, p. 101).

Furthermore, Bendiab suggest that secure and reliable IDM appears to be "the greatest challenge facing cloud computing today" (p. 724) . Although "accountability is the main construct and key enabler of trust" in the cloud (Mwenya & Brown, p. 334), "secure and reliable management of identities" is proven "the greatest challenges facing cloud computing today"(Bendiab et al., 2018, p. 724). Effective IDM in the cloud is a "key area of cloud security" and is vital for its wide adoption (Ma, 2015, p. 290; Moghaddam et al., 2017, p. 91). Still, traditional cloud-based identity and access control systems follow a centralized approach, where a cloud server acts as the central authority controlling access to data in the cloud (Sohrabi et al., 2020).

The following section discusses the development of IDM models and their attempts to address the above IDM challenges over time.

2.6. Evolvement of IDM models in addressing IDM challenges in organisations

Traditional IDM systems implement a service-centric approach, also seen as an organisation-centric approach, principally including centralized and federated IDM models. A new approach to IDM tends to be user-centric, including the so-called Self-Sovereign Identity (SSI) and some types of federated identity. (Maesa & Mori, 2020) Figure 6 illustrates the contrast between the two approaches.

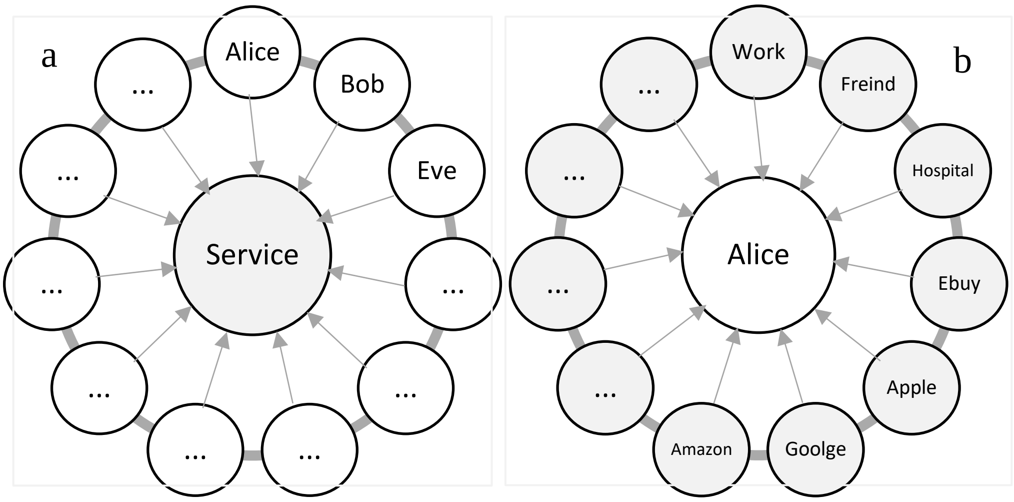


Figure 6. Service centric identity/ Traditional centralised identity (a) vs user centric identity/ Self-Sovereign Identity (b) — adapted from Maesa & Mori (2020)

2.6.1. Centralized IDM

Traditional IDM systems are “based on central authorities” usually isolated from each other, setting up silos of trust in such a way users “cannot sign on across different domains” (Bernabe et al., 2019, p. 164913). Maesa & Mori highlight that, as a result, “users are forced to rely on a different central service to manage their identity data in each different domain” (p. 105). A user has an account (username and password or biometrics) for every isolated service. Although this is virtually perfect from the enterprise perspective (since it gives an organisation complete control over the use of ‘its’ digital assets), it is “inefficient and cumbersome for users (forcing them to remember many different private authentication information)” (Maesa & Mori, 2020, p. 105). Centralised IDM systems use protocols such as Radius and Kerberos, providing authentication of both individuals and applications on a dedicated server. (Alexander, 2020).

2.6.2. ID-as-a-Service

The centralised cloud model of IDM is also called ID-as-a-Service. In this model, the organisation transfers its responsibility of managing the identities of its digital systems, including related costs, to a trusted third party. However, most organisations would prefer to manage identities themselves rather than outsourcing it as a service, mainly due to privacy issues and the legal responsibilities involved, especially in data breaches. ID-as-a-Service utilises cloud-based services protocols, usually vendor-based products, like Okta or AWS-IAM, providing authentication of both individuals and applications on a dedicated server in the cloud. (Bernabe et al., 2019; Mpofu & van Staden, 2017)

2.6.3. Federated IDM

Federated IDM is a model of trust that helps to mitigate partially the problems posed by centralized IDM by " enabling Single Sign-On (SSO)", a kind of server-centric system that "enables users to adopt the same identity system across different domains" (Alexander, 2020, p. 138-139). When signing on a trusted third party system, "the user is redirected for authentication and user identity data retrieval to his home *identity provider*" (Bernabe et al., 2019, p. 164912). In this way, the third-party's system, known as *identity consumer*, is granted some privilege on the user's identity data stored on their home central authority over the internet (Whitman & Mattord, 2018). In other words, if services A and B trust mutually, a user registered with service A can access service B without creating an account with it, and vis-versa. A typical example of a federated IDM is when a given online shopping website can be accessed using a Google account. Federation uses protocols such as OpenID, SAM, and Auth (Michael & Anna, 2019).

2.6.4. User-centred IDM.

Even though federated IDM "eases the burden on users, it still gives them no control over their identity data that remain centralized for each domain as before" (Maesa & Mori, 2020, p. 105). That is where user-centric IDM comes into play. It partially addresses privacy issues by putting the user in charge of some aspects of their own identity data, limiting the privileges of third parties. (Breuer et al., 2015). The system asks users for their consent on how much of their identity information will be "released in the federation from their home identity provider (the data controller) to the service provider (data processor)" (Bernabe et al., 2019, p. 164912). However, Bernabe et al. highlight that the user's information is still subject to a potential data breach as their “identity are still held on the server-side, and authentication is validated on the server” (p. 164912).

2.6.5. Self-Sovereign Identity (SSI)

A typical user-centric IDM uses blockchain to obtain SSI systems (Bouras et al., 2020). In this model, the decentralised identity provider system is not owned by a single entity. Thus, it “does not represent a trusted third party and allows digital identities that are under full control of the associated subject” (Grüner et al., 2019, p. 1). That is why a growing tendency portraits SSI as the most “privacy-respectful solution” for IDM systems (Bernabe et al., 2019, p. 164912). Identity data is stored on the user side, technically on their individual block, using a software wallet installed on their device (like a smartphone) (Thota et al., 2020). “Users can register, retrieve and even revoke the data if they do not want to use them anymore” (Kshetri, 2017, p. 1036).

Figure 7 below illustrates the evolvement of IDM models above discussed from the perspective of their privacy-preserving capabilities.

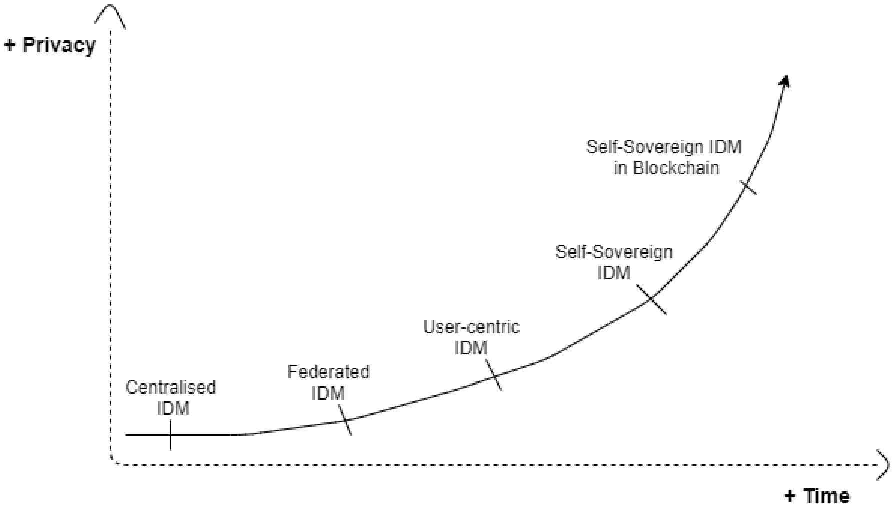


Figure 7.How IDM models have evolved from the user privacy perspective –adapted from Bernabe et al. (2019)

The following section discusses the fundamentals of blockchain and its impacting and challenging factors from the perspectives of enterprise implementation.

2.7. The blockchain technology

A blockchain is a constantly growing distributed record of updates about a specific matter among a group of participants. A consensus protocol regulates interactions among participants, and cryptographic technologies, namely digital signature and hash algorithm, maintain security (Kim et al., 2019; Post et al., 2018). Table 2 shows that blockchain implementation involves determining three fundamental needs: *who can join* the network, whether a *validator* will be needed, and what type of *consensus protocol* will regulate interactions between participants. Combining these needs results in three types of blockchain implementation: public permissionless, public permissioned, and private permissioned (Labazova, 2019; Politou et al., 2019).

Table 2. The three fundamental types of Blockchain Implementation –based on the consensus protocol, the presence of a validator, and who can join

<table>
<tr><td></td><td colspan="6"><b>Blockchain Implementation</b></td></tr>
<tr><td><i>Consensus protocol</i></td><td>Raft Consensus</td><td colspan="2">Proof of Authority (PoA)</td><td>Federated consensus</td><td>Proof of Work (PoW)</td><td>Proof of Stake (PoS)</td></tr>
<tr><td><i>Validator Trust</i></td><td colspan="4">Permissioned</td><td colspan="2">Permissionless</td></tr>
<tr><td><i>Who can join</i></td><td colspan="2">Private</td><td colspan="2">Public (Federated)</td><td colspan="2">Public</td></tr>
<tr><td><i>Description</i></td><td colspan="2"><b>Private permissioned blockchain:</b> “access authorization does not entail validation permissions, which require additional authorization rights given to several nodes”. Only trustful nodes enforce consensus.</td><td colspan="2"><b>Public-permitted</b> or <b>federated blockchain:</b> “only authenticated and predefined users can read and write transactions.
All nodes participate in the finding of the consensus.
Identifiable nodes determine consensus mechanisms”.</td><td colspan="2"><b>Public Permissionless blockchain</b>: “everyone can read, write, and validate the information. Consensus is enforced by proof-of-work or proof-of-stake. Users are usually anonymous and pseudonymous”.</td></tr>
<tr><td><i>Application</i></td><td colspan="2">Enterprise projects (Hyperledger)</td><td colspan="2">Organisational consortia (Ripple, R3)</td><td colspan="2">Cryptocurrencies (Bitcoin)</td></tr>
<tr><td><i>References</i></td><td colspan="6">(Labazova, 2019, p. 3; Politou et al., 2019)</td></tr>
</table>

2.7.1. Enterprise Blockchain (EB)

The concept of EB refers to a “permissioned blockchain utilized by any organisation” (Karamchandani et al., 2020). However, ambiguities on the applicability of EB in the real world is perhaps one of the reasons for delays in its adoption. “Technology professionals are knowledgeable, yet not enough substantial business problems have been solved with Blockchains”(Demir et al., 2020, p. 34). Demir et al. proposed the Blockchain Technology Transformation Framework (BTTF) to guide executives and managers in evaluating blockchain-based solutions to innovate their industry. Likewise, Labazova (Labazova, 2019) proposed the framework for assessing blockchain implementations in organisations, regardless of its use case. However, despite its potential impact on business that could promote its adoption, EB is still subject to various constraints.

2.7.2. Promoting and constraining factors of blockchain for an enterprise

There are eight important architectural properties of blockchain, paired in a mutual influence relation, that could promote its adoption: Decentralisation & disintermediation, programmability & automation, transparency & auditability, and immutability & verifiability (Butijn et al., 2020, p. 61:17). Additional blockchain's impacting features include integrity, origin authentication, and trust. Table 3 below discusses these architectural features of blockchain from the perspective of their business impact.

Table 3. Factors promoting the adoption of blockchain in the context of an organisation.

Blockchain Features and Business Impacts	
Decentralization & Disintermediation	Blockchain eliminates system dependencies and intermediaries (Shetty et al., 2019). It enables direct interactions between participants without the need for a trusted third party. (Butijn et al., 2020; Helebrandt et al., 2018, p. 1221).
Programmability & Automation.	Smart contracts allow for automated execution of predefined codes "once certain conditions have been met", though arbitrary code may increase bugs (Butijn et al., 2020, p. 61:17). Automation "simplify complex business processes by alleviating the need for manual interventions" (Demir et al., 2020, p. 36).
Transparency & Auditability	Each user of the blockchain can track how blocks have been added over time (El Madhoun et al., 2019). However, a permissioned blockchain might reduce transparency due to the privacy requirement (Wüst & Gervais, 2018).
Immutability & Verifiability	Blockchain keeps temper-evident historical records of all transactions happening on the network (Demir et al., 2020). "The information stored in the blocks cannot be changed unless an attacker can gather more than 51% of the computational power network" (Ahmed et al., 2019; El Madhoun et al., 2019, p. 3).
Integrity, authentication of origin & trust	Cryptographic methods ensure that information is protected from unauthorized modifications, improving trust (El Madhoun et al., 2019; Wüst & Gervais, 2018).

Blockchain is a relatively new technology that is still suffering from immaturity (Demir et al., 2020). Table 4 discusses the fundamental challenges ahead of its implementation that might prevent or delay its adoption in organisations.

Table 4. Factors constraining the adoption of blockchain in the context of an organisation

Technology Challenges	
Software and Sustainability issues	Software used to ensure transactions among active participants on a blockchain network are open-source, thus subject to frequent updates (Demir et al., 2020). Recurrent updates make the blockchain system "highly volatile" (Marsalek et al., 2019, p. 395).
Technical Integration Challenges	Due to its decentralized architecture, blockchain may make it difficult to connect with legacy systems (Demir et al., 2020). A poorly designed blockchain can result in a system incompatible with existing systems, such as "a fine-grained identity" (Marsalek et al., 2019, p. 395) and role-based access control (Upadhyay, 2020).
Scalability and performance	Blockchain requires a careful design to "ensure sufficient scalability without sacrificing decentralization" (Shetty et al., 2019, p. 14). Scalability is generally measured in throughput, latency, bootstrap time, storage, cost of confirmed transactions, fairness, and network utilization (Kolb et al., 2020).
Security	It is possible to breach the security of a blockchain "when a 'miner' controls more than 51% of the computing power" (Ahmed et al., 2019; Thai et al., 2019, p. 5). Although this is still thought very difficult to achieve, it may not be impossible with quantum computing (Fernando, 2019; Shetty et al., 2019).
Skill shortage	"Blockchain-focused technical skills are not yet taught in standard higher education curricula" (Duy et al., 2018, p. 10). As a result, the industry is suffering from a deficit of expertise. Meanwhile, the demand for blockchain skills is growing (Demir et al., 2020; Duy et al., 2018, p. 10).
Complexity	Blockchain is considered both 'user and developer unfriendly. It is thought complex to implement and difficult for a user to adapt (Lopez et al., 2019).
Business Challenges	
Cost-benefit analysis	Blockchain ecosystems were initially designed as "an investment rather than a traditional business use with an expected return on investment" (p. 37). Its upfront implementation cost is high, as it includes new infrastructure and a highly skilled team, which rather negatively impact existing revenues. (Demir et al., 2020)
Governance	"The governance of a blockchain concerning updating its fundamental rules is problematic" (Butijn et al., 2020, p. 61:19). "The whole network relies on a consensus mechanism" that involves all the nodes, " which can be any device" (Cui et al., 2020, p. 242). Therefore, there are issues of accountability and management (Upadhyay, 2020).
Uncertain regulatory status /lack of standards	The lack of firm regulatory guidelines and policy standardisation is "the most concerning challenge for bringing blockchain into many fields daily", as "laws tend to catch up slowly with new technology" (Demir et al., 2020, p. 37; Duy et al., 2018, p. 202)
Cultural adaptation and reluctance to change	The blockchain distributed fashion of sharing information "not only distributes power but also reduces the control of former authorities" and "fear of unknown technology and its possible shortcomings can cause concern." (Demir et al., 2020, p. 37)
Awareness	The widespread adoption of blockchain is also potentially restricted by the lack of adequate knowledge and awareness (Upadhyay, 2020)

These challenges tend to question the practicality of adopting blockchain-related technologies like BDIDM.

2.8. The practicality of BDIDM in organisations

This section focuses on the pragmatism of BDIDM in the context of an organisation. Among other things, the section discusses the SSI flavour of BDIDM, which was initially intended for individual use on the internet, evaluating its practicality for the enterprise context, especially the so-advertised potential to address IDM challenges in organisations.

2.8.1. The practicality of the concept of 'BDIDM for enterprise'

The following scenario sets up the context of BDIDM in organisations:

> *Alice has just joined company B. The company's system administrator, Bob, needs to create a corporate account for the newly recruited employee, Alice. A username, password, biometrics, and other personal information (such as name, physical address, phone number, national identification number, age, email address, etc.) need to be captured in the system. However, Alice already has a digital identity stored on a blockchain. Therefore, she authorises her new employer to access it without viewing her personal data. Alice can now access corporate digital resources using her Blockchain-based ID. Bob has no control over Alice's digital identity, as it is stored on an independent system. Alice has complete control over her digital identity and can authorise whatever online service she wants to create an account with, from a hospital to an online shopping website. As a result, Alice only has a single account and thus fewer passwords to recall.*

The scenario seems troublesome from the enterprise perspective of IDM for the following reasons: (i) an organisation would tend not to trust Alice's ID because it is external, (ii) it would tend to know whether the participants in that blockchain are trustworthy, (iii) it would not want to lose control over Alice's account since she has access to the company's confidential information, (iv)it would be concerned about what would happen when Alice's ID gets hacked, or whether someone is behind Alice's ID to spy the company's business. Yet, this is what BDIDM for enterprise, especially in its SSI flavour, is all about.

SSI is a paradigm focusing on a user-centric approach, an IDM model that emerged with blockchain. It "strives to place the user in full control of their digital identity" (Grüner et al., 2019, p. 1; Shetty et al., 2019). SSI is a result, on the one hand, of the decrease in users' trust in major corporations. Users are increasingly concerned about their privacy that they disapprove of the misuse of their personal data. On the other hand, "the awareness of the commercial worth of user data ownership by service providers and networking" advocates for giving back the user their power over their data. (Kuperberg, 2019, p. 2).

2.8.2. The Practicality of the BDIDM-SSI Model

Nearly the entire sample of the papers retrieved on BDIDM implementation proposals, regardless of whether they included the enterprise context, tended to converge toward the SSI as the ideal BDIDM model. They claim that SSI is decentralized and distributed (Mitani & Otsuka, 2020). Decentralization refers to the removal of the IDM central authority (server). In contrast, distribution refers to utilizing the exact copy of a user's ID across all components of the IDM system (redundancy) (Maesa & Mori, 2020).

> *Technically, SSI allows individuals to "create immutable identity records represented as identity containers capable of accepting attributes or credentials from any number of organisations. Each organisation can decide whether to trust credentials in the container based on which organisation verified or attested to them". (Maesa & Mori, 2020, p. 105)*

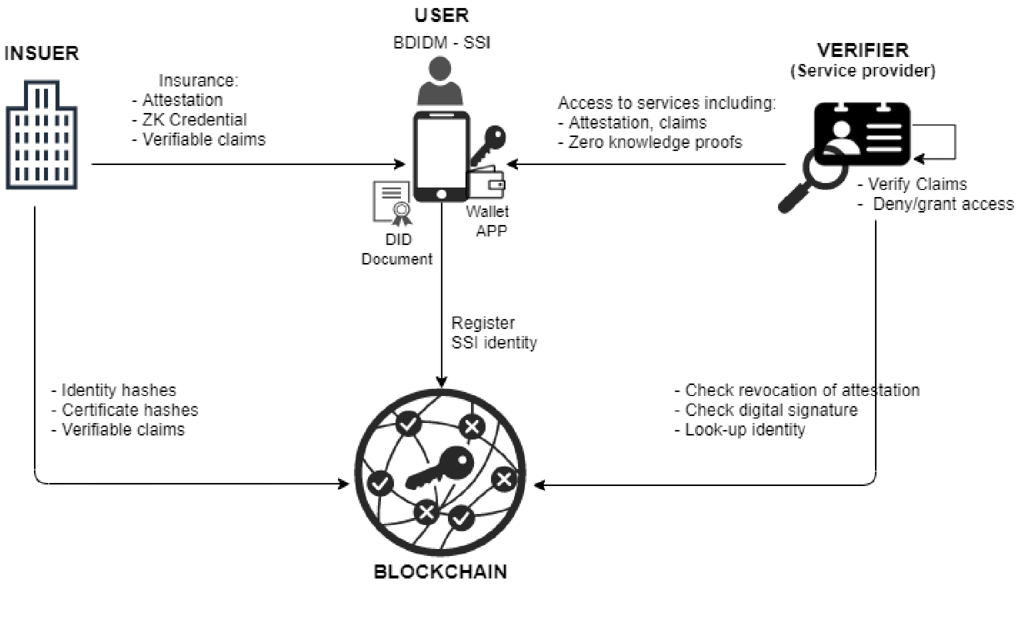


Figure 8. How Self-Sovereign identity model works. –adapted from Bernabe et al. (2019)

Figure 8 illustrates that the SSI identification process involves three parties: (i) the *subject* of the identity (user: an individual or a thing), (ii) the *certifier* or *insurance* to notarize the documents (usually “a government agency, an accounting firm or a credit referencing agency”), and (iii) the *inquisitor or verifier,* which is the service provider that “inquiries into the identity of the subject” (Kshetri, 2017, p. 1030). The user obtains a distributed identity (DID) with verifiable claims and credentials from the issuer authority, in a user-centric way using their devices such as a smartphone. The latter hosts a software wallet that keeps keys secure (Thota et al., 2020). SSI’s privacy-preserving capabilities can enable the user “to present Zero-Knowledge crypto proofs against a Service Provider acting as verifier that checks in the blockchain attestations and signatures” (Bernabe et al., 2019, p. 164913).

The principles of SSI identity include existence, control, access, transparency, persistence, portability, interoperability, consent, minimalization, and protection (Maesa & Mori, 2020). These principles could be summarised in “three characteristics usually required by any IDM system: “*Security,* the identity information must be kept secure; *controllability,* users must have control of who can access their data; and *portability*, the user must be able to use their identity data wherever they want and not be tied to a single provider” (Maesa & Mori, 2020, p. 106). The main contrast with traditional IDM systems is the control given to the user rather than to the identity provider.

However, as shown in Figure 8, a smartphone can be considered as a token authentication method, so there are still security concerns when the wallet is compromised, for example, in the event of a lost or stolen smartphone (Whitman & Mattord, 2018). Beyond this, the long-term challenge for SSI is to be resilient to the rule of 51%: a severe security breach that happens “when a ‘miner’ controls more than 51% of the computing power” (Ahmed et al., 2019; Thai et al., 2019, p. 5). This cyberattack on blockchains may still be though difficult to achieve but may not be impossible with quantum computing (Fernando, 2019; Lopez et al., 2019).

2.8.3. The Practicality of the Ideal Blockchain Implementation for an enterprise

Figure 9 shows that public permissionless blockchains, on the one hand, tend to be decentralised, transparent, scalable, but inefficient in computing power and, thus, are slow. On the other hand, private permissioned blockchains tend to be more centralised, less transparent, not scalable, but efficient in computation power consumption, thus are fast. The challenge of blockchain is that consensus algorithms, especially PoW, used to create a trustful system in a trustless environment are technically expensive to achieve. For "more efficient and simpler consensus algorithms", it is necessary to relax trust assumptions in the system, balancing between decentralisation and transparency. "The more trust a system places on nodes, "the more efficient the system gets, but often also the more centralized". (Maesa & Mori, 2020, p. 101)

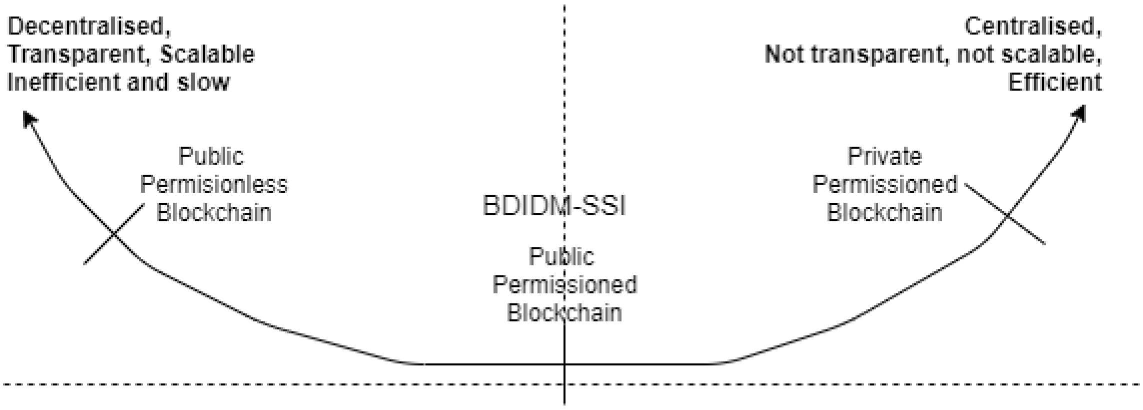


Figure 9. Balancing decentralisation and transparency to achieve efficient blockchains

Public permissioned blockchains, also known as federated blockchains, are more balanced versions of blockchains (Buccafurri et al., 2018). They tend to fit the concept of federated IDM discussed earlier and are claimed to be more decentralized, scalable, efficient (Thai et al., 2019), and ensure "privacy protection and high transparency"(Mitani & Otsuka, 2020, p. 21573). A public permissioned blockchain seems the ideal implementation for BDIDM. Indeed, Sovereign Foundation, a firm that advocates for SSI on the internet, claims to create "blockchain instances that are open for all to use" but whose network of nodes performing consensus is permissioned (Bernabe et al., 2019, p. 164911).

Still, one would argue that private permissioned blockchain may be the ideal implementation for 'enterprise BDIDM' because it endorses a service-centric approach by giving total control of the system to the identity provider called "Trust Anchor". But a service-centric approach to BDIDM would not differ from the traditional centralised IDM, from which one would want to move. "A Trust Anchor defines who represents the highest authority of a given system that has the authority to grant and revoke, read, and write access". A node with the 'Read' privilege can only view some aspects of the identity, while a node with the 'Write' privilege has full access to the identity data and can modify or even block it. (Sohrabi et al., 2020, p. 46)

Wüst & Gervais (Wüst & Gervais, 2018) proposed a structured methodology to determine the appropriate blockchain implementation to address the choice of blockchain implementation ambiguities. The methodology suggests that the choice should depend on trust assumptions. From the outsider-threat perspective of cybersecurity theory supporting traditional implicit trust (Whitman & Mattord, 2018), this means that BDIDM would be unnecessary for *trusted users* (staff members accessing the system from the intranet). That permissioned BDIDM would make sense for *semi-trusted users* (clients, suppliers, partners, etc., accessing the system from the Extranet) and permissionless BDIDM for *untrusted users* (visitors or any unknown user accessing the system from the internet).

However, with the rise of the insider-threat perspective of cybersecurity, there is a growing tendency to shift from the traditional implicit trust to a 'Zero Trust' (ZT) security architecture, as recently proposed by NIST. ZT recommend that there should be "no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)" (Stafford, 2020, p. ii). Every entity should, by default, be restricted access to the system and must accurately identify and authenticate to access it because any user is a potential threat to a digital system. In this way, ZT might endorse radical BDIDM for any user. After all, "blockchains assume the presence of adversaries in the network by making compromise significantly expensive", which is why it is claimed to create a trusted system in an untrusted environment (Shetty et al., 2019, p. XIII).

2.8.4. The practicality of BDIDM-SSI in addressing IDM challenges in organisations

SSI critics maintain its impracticality in organisations by highlighting the weakness of the blockchain that dwells at its endpoints. The anonymity of a given blockchain not only means that there is no central authority to block an account in case of identity theft or misbehaviour, but also that "each user must themselves safeguard against forgetting (or losing) the private key" (Kuperberg, 2019, p. 5). "Blockchain could practically introduce novel issues for users" because they would be the only one "in charge of managing all the cryptographic keys to protect their identity information" (Maesa & Mori, 2020, p. 106). Some researchers even question whether further adoption of blockchain-based solutions should be encouraged and whether the overall potential for change "could be net positive" (Rot & Blaicke, 2019, p. 447).

However, "reluctance to adopt disruptive technologies may be a significant competitive disadvantage for an organisation, whereas proactive planning can be a significant advantage"

(Demir et al., 2020, p. 34). Blockchain represents an opportunity for “a paradigm shift in the development of next-generation cyber defence strategies”. First, because blockchain ensures data integrity “as tampering of blockchains is extremely challenging due to the use of a cryptographic data structure and lack of reliance on secrets”. Second, because “Blockchains assume the presence of adversaries in the network, making a compromise by adversaries significantly expensive”. And third, because Blockchain “is resilient to single point of failure”. (Shetty et al., 2019, p. XIII)

Indeed, those advocating for BDIDM highlight that identity self-management could be beneficial from the privacy-preserving perspective since users have direct control of their own data. Maesa & Mori argue that identity self-management could actually “lead to the practical advantage of reduced expenses” for both users and organisations. Users because of “the potential costs of identity theft and private data leaking of traditional centralized solutions”. Organisations and external services because they “would not have to store and protect any more private information, nor replicate it among the interested services with the related costs and privacy issues”. (Maesa & Mori, 2020, p. 106)

The cost savings in password management alone could range in the millions. A Canadian study estimated that “ $572 million are lost annually to call centre password management services and lost productive hours” in the country (Wolfond, 2017, p. 38). However, critics might refute cost-saving arguments. They might suggest that the potential cost of data breaches and password management is insufficient to make a case for BDIDM in organisations, assuming that organisations would still prefer to pay those costs than the cost of losing control over users.

Elsewhere, research suggests that “blockchain-based identity and access management systems can address some of the key challenges” associated with the secure cloud (Kshetri, 2017, p. 1027). Since the IoT relies on the cloud, the “current centralized cloud model of IoT security” is problematic because “IoT devices are identified, authenticated and connected through cloud servers” that often perform processing and storage via the internet. Operations passing through the internet are subject to manipulation. “Blockchain sovereign identity solutions’’ can help solve these issues, and some projects and experiments that focus on IoT identity problems are undergoing (Zhu & Badr, 2018, p. 1568)

A pragmatic point of view would argue that the disruptive capabilities of BDIDM may be beneficial “only in those scenarios where the advantages outweigh the drawbacks” (Maesa &

Mori, 2020, p. 99). In other words, when considering a benefit of BDIDM, such as privacy-preserving, one “should question whether it would add value, eliminate a weakness, provide an advantage, or preclude a threat from competitors”(Demir et al., 2020, p. 36).

Still, an objective viewpoint would add that more empirical evidence is needed to prove the prevailing argument. Hence the criticality of understanding the theoretical considerations surrounding the adoption of BDIDM in organisations.

2.9. Theoretical considerations about the adoption of BDIDM in organisations

This section analyses how related theories would shape the adoption of BDIDM in organisations. The section identifies the Technology-Organisation-Environment theory as more suitable for explaining this matter than other competing theories. The section ends by proposing a revised version of the TOE, called TOE-BDIDM, as a research model for future empirical studies.

2.9.1. Learning from related empirical studies

Some studies have recently studied the adoption of blockchain technology, mainly in its use case of supply chain management. Unlike Kamble et al. (2019) and Queiroz and Wamba (2019)’s studies that were based on individual blockchain adoption, this study considers the enterprise perspective of blockchain adoption like those by Clohessy and Acton (2019) and Karamchandani et al. (2020). Nevertheless, all of these studies used one or a combination of the Technology Acceptance Model (TAM), the Theory of Planned Behaviour (TPB), the Unified Theory of Acceptance and Use of Technology (UTAUT) and the Technology Readiness Index (TRI) frameworks.

Since this study focuses on a single blockchain’s use case of IDM in the context of an enterprise, the TOE theory seemed appropriate. Initially described by Tornatzky & Fleischer in 1990 as part of ‘The Processes of Technological Innovation’ and lately updated by Jeff Baker in 2011, TOE is a framework that defines enterprise-level theory, explaining how the firm context impacts the adoption of innovation (Baker, 2012).

Unlike some studies limiting the framework to the organisational element only, considering it “the most significant determinant of IT innovation adoption in organisations” (Clohessy &

Acton, 2019, p. 1457), this study considers the entire TOE framework. Karamchandani et al. (2020) recommended introducing a technological perspective. In addition, the three elements of technology, organisation, and environment constitute a full context of an enterprise. They have been shown to impact, by constraining or promoting, how an organisation "identifies the need, searches, and adopts new technologies" (Baker, 2012, p. 232).

2.9.2. Technological context

The technological context consists of an organisation's technologies in use and those existing in the marketplace but not yet adopted. Technologies in use impact the organisation's adoption decision by determining the scope boundaries and the extent to which technological change is needed. Innovations that exist but have not yet been adopted impact the adoption decision making of the organisation by setting the limits of what is possible and illustrating how technology can enable the organisation to evolve and adapt. (Baker, 2012)

Existing technologies like centralised access control may play a key role in adopting BDIDM as they may not be compatible with a distributed architecture (Marsalek et al., 2019). However, some BDIDM product vendors (such as IBM, KYC-Chain, UniquID, Microsoft, Oracle, etc.) are now available on the market. Organisations can gain some insight into what it could be possible to achieve and what it could not. Nevertheless, BDIDM is disruptive, a kind of 'radical' innovation, as it may render existing IDM and related competencies obsolete. In contrast to innovations that bring incremental or synthetic change, BDIDM does not "introduce new versions of existing technologies" but tends to replace existing centralised IDM systems by "combining existing technologies" in a radically different manner of distributed computing (Baker, 2012, p. 232). Blockchain tends to shift the security paradigm by assuming "the presence of adversaries in the network" (Shetty et al., 2019, p. XIII). Therefore, as part of what Baker describes as "innovations that produce discontinuous change", BDIDM has a high adoption risk. Still, it may have the potential to "enhance competitive standing in an organisation" (232).

From an InfoSec perspective, Hameed and Arachchilage (2020) identified additional technology characteristics that impact the adoption of innovation in enterprises, which are also relevant to the adoption of BDIDM: trialability (Ease with which the user would adapt/appreciate BDIDM), observability (Degree of controllability and monitoring of BDIDM by an organisation), compatibility (Ease with which the BDIDM system would interoperate with other systems), and complexity (Ease with which an organisation would implement BDIDM). In addition to these, another relevant technological construct is “Technical know-how” (Awa et al., 2016, p. 7), which includes the availability of skills, consultants, vendors, etc. However, Baker (2012) identifies these items under External Environment instead.

2.9.3. Organisational context

The organisational context consists of firm characteristics and resources that can impact adoption in different ways.

The first is the organisation structure: formal mechanisms linking different units of the organisation (internal boundaries) may promote innovation. Virtually, organisations with an organic and decentralized organisational structure may be suited for the BDIDM adoption phase. Those with formal reporting relationships, centralized decision-making, and clearly defined roles for employees may be the best in the implementation phase. (Baker, 2012)

The second is the organisational communication processes, which may either promote or constrain adoption. Support from top management is key to preparing a corporate culture that welcomes change. The support includes describing the role of innovation within the organisation's overall strategy, indicating its importance to subordinates, rewarding initiatives, and building “a skilled executive team” that can cast a compelling firm vision (Baker, 2012, p. 233). Regarding BDIDM, since organisations tend to be hostile to privacy, “top management support and organizational readiness are enablers for the adoption of Blockchain” (Clohessy & Acton, 2019, p. 1457).

The third is the organisation's size, considered minor requirements as there have not been many empirical studies that confirm their link to innovation adoption (Baker, 2012). Instead, the financial cost is reported to have a significant impact. This may be relevant for BDIDM adoption, as BDIDM is perceived to be relatively expensive to implement (Demir et al., 2020), both in terms of finance and human competencies. However, some studies on blockchain show that large enterprises would be more likely to adopt BDIDM than SMEs (Clohessy & Acton, 2019). Besides, Cultural adaption, awareness, and reluctance to change may also impact the adoption of BDIDM (Upadhyay, 2020).

2.9.4. Environmental context

The environmental context is all about the industry's structure (such as competition, dominant firms, etc.), whether technology service providers and the regulatory environment (such as government regulations) exist. For instance, the industry life cycle impacts innovation adoption: firms in rapidly growing industries tend to innovate more quickly than those in mature or declining industries. Similarly, the support infrastructure for technology, the availability of skills, labour and consultants, and government regulation impact adoption. (Baker, 2012)

Concerning BDIDM, government regulations in the field of IDM (such as the legal requirement for organisations to protect user privacy, case of POPIA in South Africa), standards (such as codes of best practices, like ISO/IEC and NIST), and cyber-threat landscape; could impact BDIDM adoption in organisations (Grassi et al., 2017; Liu et al., 2019). However, blockchain still lacks firm regulatory guidelines and policies for standardisation (Demir et al., 2020; Duy et al., 2018).

2.9.5. The TOE-BDIDM Research Model

Figure 10 below illustrates TOE-BDIDM, the proposed research model to empirically investigate the TOE factors affecting the adoption of BDIDM in organisations. TOE-BDIDM is rooted in the TOE theory as described above, a revision of the original model proposed by Baker (Baker, 2012). The revision aimed to adapt the TOE model to the InfoSec and blockchain contexts. For example, the items 'Readiness' and ‘Awareness’ were added due to the relative newness of the blockchain (Demir et al., 2020; Upadhyay, 2020). Governance and standardisation of the blockchain would also impact the decision to adopt BDIDM in organisations (Butijn et al., 2020). The literature shaped addition items, including Security, Privacy, Competencies, and Skill Labour. The BDIDM Type variable was added under BDIDM characteristics to measure the type of blockchain implementation an organisation would prefer for BDIDM adoption.

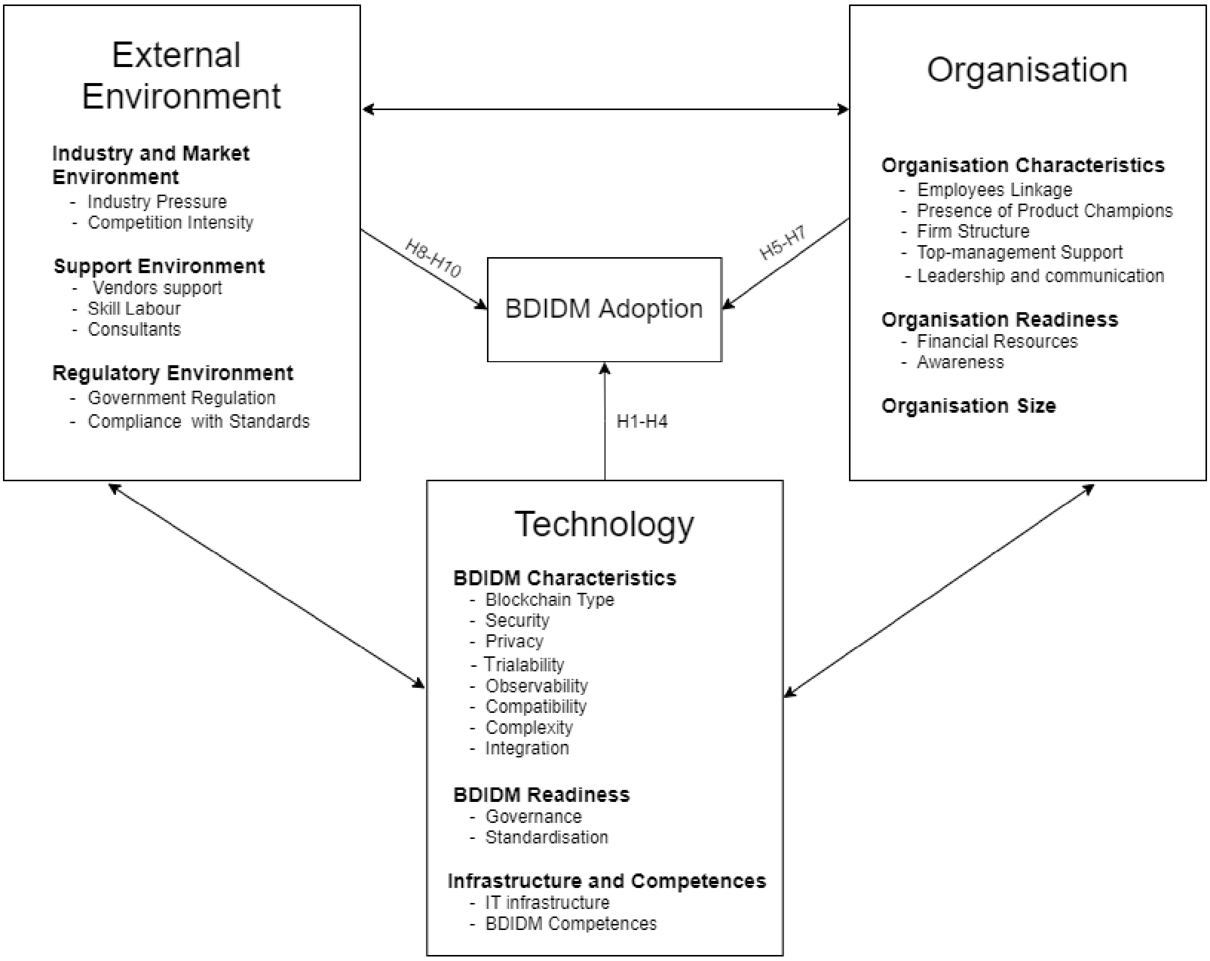


Figure 10. The TOE-BDIDM model. A contextualised version of the TOE model by Baker (2012)

Following are the study's Alternative Hypotheses (H_a) embedded in the model:

Ha_1: BDIDM Characteristics have a statistically significant impact on BDIDM Adoption in organisations.

Ha_2: Statistically, Blockchain Types are significantly different and therefore are associated with BDIDM adoption in organisations.

Ha_3: BDIDM Readiness have a statistically significant impact on BDIDM Adoption in organisations.

Ha_4: IT Infrastructure and Competencies have a statistically significant impact on BDIDM Adoption in organisations.

Ha_5: Organisation Characteristics have a statistically significant impact on BDIDM Adoption in organisations.

Ha_6: Organisation Readiness has a statistically significant impact on BDIDM Adoption in organisations.

Ha_7: Statistically, Organisation Sizes are significantly different and therefore are associated with BDIDM adoption in organisations.
Ha_8: Industry and Market Environment have a statistically significant impact on BDIDM Adoption in organisations.
Ha_9: Support Environment has a statistically significant impact on BDIDM Adoption in organisations.
Ha_{10}: Regulatory Environment has a statistically significant impact on BDIDM Adoption in organisations.

2.10. Chapter summary

This section synthesises what was discussed throughout the chapter considering the review objectives and scope introduced earlier. Among other things, the review objectives embedded the study's argument of the practicality of BDIDM for the enterprise being questionable. On the one hand, the review tacitly demonstrated whether the claims made about blockchain, including its potential to address IDM challenges in organisations, were as factual as the study assumed. On the other hand, it implicitly showed whether BDIDM was as disruptive for organisations (compared to traditional IDM systems) as the study assumed. The section ends by highlighting several knowledge gaps identified in the literature as hints for further research.

2.10.1.Review synthesis

This review sought to explore the literature to provide background on the IDM use case of blockchain. The aim was to understand the topic, mostly how practical the adoption of BDIDM was from an organisational perspective, especially its ability to address IDM challenges. The review introduced several claims about Blockchain and BDIDM to see if they had any theoretical foundation. The main review findings could be synthesised as followed:

First, IDM consists of managing matters related to two fundamental InfoSec principles: identification and authentication. Identification labels each entity with an identifier, while authentication allows it to prove they are who they claim to be. IDM is essential because a system should grant access only to legitimate users. IDM can be implemented in two traditional approaches: Centralised or federated IDs. A new approach to IDM implementation is distributed IDs (which include the SSI model). The critical challenges of IDM to be addressed include (i) vulnerabilities in authentication methods, (ii) vulnerabilities in IDM architecture,

(iii) the balance between security and privacy, (iv) credential reuse and weak credentials, and (v) Secure-Cloud and Secure-IoT.

Second, a blockchain is a continuously growing distributed record of updates about a specific matter, such as IDM. A consensus protocol regulates interactions among participants, and the security of data is maintained using cryptography. A blockchain can be implemented in three fundamental ways: public permissionless, public permissioned, and private permissioned. The literature suggests two guidelines to help an enterprise leverage blockchain: Blockchain Technology Transformation Framework and Framework for Evaluation of Blockchain Implementations. When doing so, enterprises should consider, on the one hand, five business-promoting factors linked to its features: (i) Decentralisation and disintermediation, (ii) programmability and automation, (iii) transparency and auditability, (iv) immutability and verifiability, (v) integrity, authentication of origin, and trust. On the other hand, 11 business and technological challenges linked to its implementation: (i) Software and sustainability, (ii) Technical integration, (iii) scalability and efficiency, (iv) security, (v) skill shortage, (vi) complexity, (vii) cost-benefit analysis, (viii) governance, (ix) uncertain regulatory status and lack of standard, (x) Cultural adaption and awareness, and (xi) reluctance to change

Third, blockchain is the underlying technology used to implement a typical distributed IDM system known as SSI. Blockchain does not eliminate vulnerabilities in authentication methods or prevent users from reusing credentials or using weak ones. However, blockchain mitigates the risks linked to vulnerabilities of authentication methods due to cryptography, providing an extra security layer in addition to MFA. Moreover, thanks to its distributed architecture, its decentralised and disintermediation proprieties, blockchain may not have SPOF vulnerability as traditional centralised systems do. BDIDM might also mitigate credential reuse as it allows for ID interoperability among different services, thus significantly reducing the number of accounts per user. Additionally, BDIDM-SSI might better preserve user privacy as it enables them to self-manage their identity data, thus mitigating risks linked to data breaches. Lastly, BDIDM could potentially help achieve secure cloud and secure IoT.

Fourth, an enterprise might implement BDIDM using a public permissioned blockchain to take advantage of blockchain disruption. It turned out that that public permissioned blockchain tends to be ideal for SSI implementation. SSI follow three fundamental principles. (i) Security, identity data must be kept secure; (ii) Controllability, users must control who can access their data; and (ii) Portability, the user must be able to use their identity data wherever they want to. Although a private permissioned blockchain would fit the current enterprise IDM context, it would not differ from the traditional centralised IDs from which one might want to move. A traditional cyber threat theory suggests that the choice of BDIDM implementation should depend on the trust assumptions. NIST highlights the new tendency to shift from this traditional implicit trust to zero-trust security architecture. If widely adopted in organisations, Zero Trust could enable BDIDM diffusion because it assumes that all users are untrusted, exactly what BDIDM-SSI advocates for. In the meantime, when adopting BDIDM to manage identities in an enterprise, one should consider doing a Strength-Weaknesses-Opportunity-Threat analysis according to their business context.

Last, on the debate on whether to adopt BDIDM in organisations, supporters argue that user privacy matters even in an organisational context, which often prioritises security over privacy. Supporters see the potential of blockchain to mitigate IDM challenges, including cost-saving on the daily IDM maintenance due to the SSI's identity self-management feature, hence may decrease data breaches. However, critics of BDIDM would refute this, arguing that organisations would still prefer to pay the cost of corporate IDM than lose control over users. Since empirical evidence is crucial to prove the prevailing argument, the review identified the TOE as more suitable to empirically investigate this matter. The TOE explains how the firm context, in terms of technological, organisational, and environmental contexts, impacts the adoption of innovation like BDIDM. The TOE model was revised to adapt it to the BDIDM context. Hence, the TOE-BDIDM research model is proposed for further empirical studies.

In summary, most of the claims about blockchain and BDIDM discussed in the review appeared to have some theoretical foundation. This verified the study's assumption that claims about blockchain, including its potential to address IDM challenges in organisations, were factual rather than just a result of hype. Therefore, one could infer that a carefully designed and implemented BDIDM will potentially mitigate IDM challenges, probably reduce the cost related to daily identity maintenance, and possibly decrease data breaches in organisations. Although BDIDM-SSI might not fully make sense to organisations yet, as assumed by the study and as apparent through the literature discussion, proactive planning instead of ignorance or resistance could avoid potential competitive disadvantages in the future. Ultimately, more research is needed to get blockchain to move from theory to practice by solving real-world issues like IDM challenges. Hence, the proposed TOE-BDIDM research model to guide further study

2.1.1. Gaps in the literature

While reviewing the selected papers, the researchers observed some knowledge gaps at different levels that might inspire future research.

First, there is a lack of blockchain standards, regulations, and guidelines. Some studies (Demir et al., 2020; Labazova, 2019) have partially addressed the guidelines aspects. However, more studies are needed to fill in the gap of blockchain standardisation, as it seems to be one of the potential precursors of its adoption and diffusion in organisations.

Secondly, most papers retrieved about nonfinancial blockchain are either generic or mainly focused on the supply chain use case. The few materials dedicated to Blockchain IDM specifically discussed the topic from the perspective of IoT (Identification and authentication of smart devices on the internet), Cloud computing perspective (ID-as-a-Service), or the individual adoption (adoption of blockchain ID by individuals for internet use). Very few included or were about the enterprise perspective.

Thirdly, most of the retrieved papers about the IDM use case of blockchain are conceptual than empirical. Empirical studies on blockchains are still rare, partially justified by the newness of blockchain. Although conceptual works are equally important, more should be done, including investigating BDIDM through empirical studies.

Lastly, of the empirical studies on blockchain retrieved, none was about blockchain-based ID management. In addition, they all used one or a combination of TAM, TPB, UTAUT, and TRI. Researchers found only one study that included only one construct of the TOE theory. Additionally, none of them had tested the TOE theory quantitatively. Some used TOE with qualitative methods (Clohessy & Acton, 2019), while others used quantitative methods with different theories (Queiroz & Wamba, 2019).

CHAPTER 3: RESEARCH DESIGN AND METHODOLOGY

3.1. Introduction

This chapter discusses the methodological framework followed in undertaking this research. Since the research topic felt under InfoSec Management, a subset of Information Technology Management, Saunders' Research Onion guided the research design and methodology. The latter is a well-known research methodology framework intended to guide business and management researchers in their research design and methodological choices. As its name suggests, Saunders' Research Onion pictures research as an onion whose layers represent different design levels involved in the research process. The core part concerns the techniques and procedure of data collection and analysis. The idea is that to reach the core part, one must peel the top layers first, just as it happens with a real onion in the kitchen (Saunders et al., 2016). The following sections discuss different layers of the research design and methodology, from the research philosophy (the topmost layer) to techniques and procedures of data collection and analysis (the core part).

3.2. Research philosophy

Saunders et al. define the research philosophy as " a system of beliefs and assumptions about the development of knowledge" (2019, p. 130) since the prime objective of any research is to develop knowledge in a field. Further on, they suggest that a research philosophy is mainly expressed in terms of ontology, epistemology, and axiology.

3.2.1. Ontology

Ontology is concerned with assumptions about the nature of the reality being studied. Saunders et al. suggest two ontologies mainly used in business and management research: *objectivism* and *subjectivism.* Both are accepted as producing valid knowledge by many researchers, even though they function based on opposing assumptions. Objectivism assumes that "social entities exist in reality external to social actors concerned with their existence". In contrast, subjectivism assumes that "social phenomena are created from the perceptions and consequent actions of those social actors concerned with their existence". (Saunders et al., 2019, p. 110)

This research was driven by an *objectivism* ontology because identity management is an objective entity: universal, based on fact, and independent from the context. For instance, if a server storing identity data is set with a weak password, like "12345678", since it is interconnected with other networks (including the internet), it is exposed to a potential data breach independent of its owner and location (Alexander et al., 2020). InfoSec practitioners often operate based on pre-established structures and procedures that generally comply with a set of information and cybersecurity global standards and regulations (Grassi et al., 2017; Liu et al., 2019; Whitman & Mattord, 2018).

3.2.2. Epistemology

Epistemology is concerned with assumptions about "what constitutes acceptable knowledge in a field of study". Two main philosophies shape what one considers as acceptable knowledge about a phenomenon: *Interpretivism* and *positivism.* Apart from these, Sunder Interpretivism tends to support subjectivism and is more concerned with 'feelings', 'attitudes', etc., of social entities toward the phenomenon studied. It tends to examine 'details' to find "subjective meaning" necessary to understand the phenomenon. Positivism tends to support objectivism and is more concerned with facts and the credibility of data. It argues that "only observable phenomena provide credible data, facts" therefore are "less open to bias". (Saunders et al., 2019, p. 112)

Apart from these, Saunders et al. consider other philosophies used in business and management research representing less radical positions: *realism* and *pragmatism.* Realism reflects assumptions from both positivism and interpretivism. In addition to supporting that "observable phenomena provide credible data, facts", realism assumes that "insufficient data means inaccuracies in sensations" (*direct realism*) and that a "phenomenon create sensations which are open to misinterpretation" (*critical realism*). Pragmatism tends to avoid the philosophical debate by focusing on what best help to answer the research question. It considers that "either or both observable phenomena and subjective meanings can provide acceptable knowledge dependent upon the research question". (Saunders et al., 2019, p. 119)

This research considered the philosophy of *positivism* in the instance of the *natural scientist.* The BDIDM adoption in organisations is a reality that exists independently of social actors (In this case, information and cybersecurity practitioners) and can be observable using objective methods. Saunders et al. (2019) state that positivists "prefer working with observable social reality and that the end product of such research can be law-like generalisations" (p. 19). This means when observing Information and cybersecurity practitioners' opinions about BDIDM adoption in their respective organisations, the researcher focused on what could be objectively quantified (in this case, the extent of their opinions) based on facts (the statements in the survey questions) and without interference. This reasoning reflects an *etic* approach as researchers were outsiders and did not directly engage with participants (for instance, through interviews). Data was collected objectively and quantitatively based on an instrument generated using existing theory to test hypotheses. From the results, some conclusions were drawn to the population.

3.2.3. Axiology

Axiology is concerned with assumptions about the degree and ways researchers' own values and participants' influence the research process (Saunders et al., 2019). In this study, as positivists, the researchers were concerned with the objectivity of the results that they attempted to not compromise it with their own or participants' bias. The researchers believe that social actors exist independently of each other and the phenomenon being studied.

3.3. Approach to the theory development

There are two main research approaches to developing a theory: *Inductive* and *deductive* reasoning. Inductive reasoning is a bottom-up approach that moves from a more specific to a broader explanation. In contrast, deductive reasoning is a top-down approach that goes from more general to more specific. Inductive reasoning aims to build a new theory, while deductive reasoning tests an already existing theory. (Saunders et al., 2019)

This study opted for *deductive* reasoning since it aimed to test whether the TOE theory is verified in the context of BDIDM adoption in organisations. Baker (2012) claims that TOE has "broad applicability and possesses explanatory power" (p. 151) across various technological, industrial, and national/cultural contexts. They add that TOE factors have been proven to influence how an organisation "identifies the need for, searches for, and adopts new technology" (p. 232). Part of the objectives of this research was to attest whether these claims applied to the context of adopting BDIDM in organisations.

However, the initial exploration tended to be inductive as it sought to understand the topic, including how practical BDIDM was from the enterprise perspective. It explored underlying facts that could explain some of the literature's claims, including BDIDM's ability to address IDM challenges in organisations. It used Meta-synthesis, a strategy rooted in an interpretive approach to “rigorously synthesize qualitative” literature to produce generalisable knowledge. (Walsh & Downe, 2005, p. 208-209).

3.4. Methodological choice

Choice of data collection and analysis methods is all about whether to use (i) mono-method: either a quantitative or a qualitative method, (ii) multiple methods: either multiple quantitative or multiple qualitative methods, or (iii) mixed methods: both quantitative and qualitative methods (Saunders et al., 2019).

This research utilised only quantitative methods of data collection and analysis; thus, it is mono method. The questionnaire was designed quantitatively to enable statistical analysis, testing the hypotheses embedded in the TOE. The choice of quantitative methods was motivated by the study’s objective and the need to address a methodological gap in the literature. None of the retrieved empirical studies about Blockchain adoption has tested the TOE theory quantitatively. Clohessy & Acton (2019) used TOE with qualitative methods, while Queiroz & Fosso Wamba (2019), Kamble, et al. (2018), and Karamchandani et al. (2020); used quantitative methods but with different theories.

3.5. Research strategy

There are various research strategies for conducting business and management research depending on the purpose of t as research —which can be exploratory, descriptive, prescriptive, or explanatory. The most common are *experiment, survey, case study, action research, grounded theory, ethnography,* and *archival research*. (Saunders et al., 2019).

Experiments are rooted in natural science and laboratory-based research, which is often explanatory, especially studying causal relationships among variables. Experiments are very rigorous, “often seen as the ‘gold standard’ against which the rigour of other strategies is assessed” (p. 178). Surveys are “popular and common” in “business and management research and are most frequently used to answer who, what, where, and how questions” (p. 181). Surveys are often associated with the deductive approach and tend to be exploratory and descriptive. A case study is “an in-depth inquiry into a topic or phenomenon within its real-life setting” (p. 184) and can adapt to both deductive and inductive approaches. Grounded theory is often viewed as the best example of the inductive approach, even as it builds a theory by combining both induction and deduction. Ethnography is also rooted in the inductive approach, originating from the anthropology field and aims at describing and explaining a social phenomenon in the way research subjects inhabit would describe and explain it. Archival research simply uses administrative records and documents, including digital archives, as the principal source of data. (Saunders et al., 2016).

This study utilised the survey strategy because it dealt with ‘what’ and ‘how’ research questions. Moreover, its purpose was both descriptive and explanatory and used a deductive approach to theory building. The study was not casual and, therefore, would not benefit from an experiment. Moreover, a survey was successfully used with the TOE framework by Awa et al. (2016). In a survey, especially using questionnaires, the researcher does not need to engage directly with participants like is the case with interviews in a case study. This helped prevent the researchers from interfering with the research in alignment with the ontological and epistemological assumptions. A case study would not align with the research philosophy as it would bind the study to a single context (Saunders et al., 2019) and make the generalisation task even more difficult.

The initial exploration that aimed at understanding the topic used a strategy of literature review, called meta-synthesis review, a “qualitative meta-aggregation and meta-summary” research methodology that seeks to summarise and “distil information to draw conclusions” (Finfgeld-Connett, 2018, p. 10-11)

3.6. Time Horizon

Research can be conducted in a *cross-sectional* or *longitudinal* manner. Cross-sectional studies are conducted over a short period, like days, weeks, or months. In contrast, a longitudinal study is conducted over a more extended period and involves collecting data on multiple points to understand a phenomenon using a different set of data. That is why longitudinal research tend to be expensive than a cross-sectional study. (Saunders et al., 2019)

Due to limited resources, this study followed a cross-sectional time horizon. The data were collected only once and not multiple times. There was no need for different tests at a different stage of the research, like in experimental studies. Hence, a longitudinal study was not appropriate.

3.7. Techniques and procedures of data collection

Since the positivism paradigm was adopted, the data collection instrument consisted of a questionnaire, specifically an *online questionnaire,* to prevent researchers interferences. Since an objectivism ontology drove the research, only *close-ended questions* were used to collect quantitative data, yielding accurate and objective results.

3.7.1. Research population and sample

A population is an entire group to which a study generalise the results, while a sample is a specific group within the population from which data is collected. In different words, the population is "the full set of cases or elements from which a sample is taken" (Saunders et al., 2016, p. 274).

The targeted population to which this study attempted to generalise the results consists of *every organisation in the world.* This study felt under information and cybersecurity management matters which are universal and tend to be independent of the geographical context. Thus, the unit of analysis of this study was organisation, while the unit of observation was information and cybersecurity practitioner.

Since it was unrealistic for this study to conduct a census by collecting data from the entire population (Saunders et al., 2016), the research sample consisted of *South African organisations* only. The choice was motivated by both South Africa's proximity to researchers and high exposure to data breaches. As discussed in the literature review chapter, data breaches are a core issue related to the IDM challenges. Africa is considered to have one of the highest numbers of cybercrimes and financial losses (Musuva-Kigen et al., 2016). The IBM 2019 Cost of a Data breaches Study reported an increase in the average cost of a data breach in South Africa by 12% from 2018 to 2019 (IBM-Security, 2019), predicted to increase with the COVID-19 impact.

3.7.2. Sampling methods, sample frame and size

There are two categories of sampling methods: *probability sampling* (also called representative sampling) and *non-probability sampling* (also called judgemental sampling). Probability sampling requires some extents of randomness in choosing participants than non-probability sampling. With probability sampling, the participants have an equal chance to be selected from the population, which is not the case with non-probability sampling. Thus, probability sampling techniques are considered more objective and are often associated with surveys and experimental research strategies. Probability sampling includes sampling techniques like *simple random, stratified random, systematic, and cluster*. Non-probability include sampling techniques like *quota, snowball, convenience, purposive, and self-selection*. (Saunders et al., 2016)

This research chose an arguably non-bias sampling method of probability sampling and simple random as sampling technique. This aligned with the selected strategy survey and preserved the objectivity of results. Moreover, participants had an equal chance to be selected and were chosen at random.

A sample frame is “a complete list of all the cases in the target population” (Saunders et al., 2016, p. 277) from which the sample was drawn. In this study, the sample frame consists of *InfoSec practitioners*, especially those working in the identity and access management (IAM) field but not limited to these. The research considered most of the population characteristics to ensure the representativeness of the sample. The sample frame consisted of different managerial levels of information and cybersecurity management, as generally classified based on both ISO/IEC and NIST standards (Alexander, 2020; Whitman & Mattord, 2018):

- Chief Information Security Officer (CISO), Chief Information Officer (CIO), Chief Technology Officer (CTO), etc.: They lead digital transformation and set the information security policy in an organisation. They might play a decisive role in the adoption of BDIDM in their respective enterprises.
- Security managers: They are responsible for the security of a specific area of the organisation, such as a building or a department (E.g., ICT, Accounting, etc.). They might have distinct perceptions of BDIDM adoption.
- Technical staff —such as system administrators, cybersecurity analysts, Identity and Access Management (IAM) administrators, etc.: They are responsible for implementing, maintaining, and monitoring security measures according to the InfoSec policy. They might have a pragmatical perspective of BDIDM adoption.

The targeted sample size was 300 valid responses, an ideal for quantitative analysis like structural equation modelling and regression (Kyriazos, 2018). However, the actual sample size was heavily constraint by the time frame (which was subject to the academic calendar), lack of funds for an intensive data collection, the responsiveness of participants (InfoSec practitioners tend to be ‘reserved’ due to the ‘confidential’ aspects linked to their job (Whitman & Mattord, 2018), and most unexpectedly the impacts of COVID-19 pandemic.

3.7.3. Data collection instrument: Operationalisation of the TOE framework

The data collection instrument was rooted in the TOE-BDIDM model, as discussed in the literature review. Table 5 defines the principle measurements retain in the final instrument. The table also gives the type of scales used to observe them, indicating a combination of nominal (variables with three to four categories and variables with ‘Yes/No’ values (binary)) and intervals (Linkert scales of 5 values: from 1 for ‘Strongly disagree’ to 5 for ‘Strongly agree’).

Table 5. Descriptions of the principle measurements of the BDIDM model

	Label	Name	Definition	Reference	Scale Type
Technology	**BDIDM Characteristics:**	**BDIDM_Char**		**(Baker, 2012, p. 232)**	
	Security (Sec)	Conf	Confidentiality: Resilience to unauthorized view (Whitman & Mattord, 2018)	(Michael & Herbert, 2017; Thai et al., 2019; Fernando, 2019)	Interval
		Int	Integrity: Resilience to unauthorized change		Interval
		Avail	Availability: Accessibility to users when needed		Interval
	Blockchain Type1	Type1	Blockchain implementation type	(Labazova, 2019)	Nominal
	Blockchain Type2	Type2	Blockchain implementation type		Nominal
	Trialability	Trial	Easiness of use	(Hameed & Arachchilage, 2020)	Interval
	Complexity	Cplex	Easiness of implementation	Hameed and Arachchilage (2020); (Lopez et al., 2019).	Interval
	Observability	Obs	Easiness of being controlled	(Hameed & Arachchilage, 2020)	Interval
	Compatibility	Cpat	Easiness of interoperability	(Hameed & Arachchilage, 2020)	Interval
	Integration	Itegra	Rate of smoothly functioning in an ecosystem	(Marsalek et al., 2019)	Interval
	BDIDM Readiness:	**BDIDM_Read**		**(Baker, 2012, p. 232)**	
	Technology Readiness	Tread	BDIDM preparedness for Enterprise context	(Demir et al., 2020)	Interval
	Standardisation	Std2	BDIDM normalisation	(Demir et al., 2020, p. 37; Duy et al., 2018, p. 202)Demir et al., 2020)	Interval

	Infrastructure and Competences:	**Infr_Comp**		**(Baker, 2012, p. 232)**	
	Competences	Cpet	Availability of BDIDM competences	(Awa et al., 2016; Duy et al., 2018)	Interval
	IT infrastructure	ITInf	Availability of IT infrastructure supportive of BDIDM	(Baker, 2012, p. 232)	Interval
Organisation	**Organisation Characteristics:**	**Org_Char**		**(Baker, 2012, p. 232)**	
	Employees Linkage	Net	formal and informal employees networking supportive of BDIDM	(Baker, 2012, p. 232)	Interval
	Presence Product Champion	Cham	availability of perceptions of BDIDM value	(Baker, 2012, p. 232)	Interval
	Top management Support	MSup	Strategic support and planning for BDIDM	(Baker, 2012, p. 232)	Interval
	Leadership and Communication	Com	Strategic communication about BDIDM values	(Baker, 2012, p. 232)	Interval
	Organisation Readiness:	**Org_Read**		**(Baker, 2012, p. 232)**	
	Organisation Financial Readiness	ORead	Preparedness for financial investment in BDIDM	(Baker, 2012; Demir et al., 2020)	Interval
	Awareness1	Awa1	Awareness of BDIDM	(Upadhyay, 2020)	Interval
	Awareness2	Awa2	Awareness of BDIDM	(Upadhyay, 2020)	Interval
	Organisation Size	**Size**	**Type of enterprise/Number of employees**	**(Baker, 2012, p. 232)**	**Nominal**
Environment	**Support Environment:**	**Sup_Env**		**(Baker, 2012, p. 232)**	
	Vendor Support	VSup	BDIDM products vendors support	(Baker, 2012, p. 232)	Interval
	Skill Labour	Slab	BDIDM external skills support	(Baker, 2012, p. 232)	Interval
	Consultants	Cons	BDIDM consultants support	(Baker, 2012, p. 232)	Interval
	Market and Industry:	**Ind_Mark**		**(Baker, 2012, p. 232)**	
	Industry Pressure	Ind	Industry pressure for BDIDM adoption	(Baker, 2012)	Interval
	Competition Intensity	Cpeti	BDIDM adoption competition gains	(Baker, 2012)	Interval
	Regulatory Environment:	**Reg_Env**		**(Baker, 2012, p. 232)**	
	Government Regulation	Gov	Government pressure for BDIDM adoption	(Demir et al., 2020; Duy et al., 2018)	Interval
	Compliance with Standards	Std2	Pressure for BDIDM adoption to comply with standards	(Grassi et al., 2017; Liu et al., 2019).	Interval
Adopt Indicator		**Adopt**	**Adoption intention**	**(Baker, 2012)**	**Nominal (Binary)**

Every item was translated into a specific survey question, depending on its scale type, which made up the online questionnaire built using Microsoft Forms. The late is a cloud-based platform that allows a convenient flow throughout a questionnaire in a user-friendly format. Microsoft Forms stores data on a cloud, accessible in a spreadsheet format usable on any data analysis software. All questions were close-ended. The questionnaire was subdivided into three sections representing the TOE model's contexts making up the dependants variables: Technology, Organisation, and Environment. The fourth section consisted of the dependent variable, BDIDM Adoption. An additional section was added to capture some background information about the sample. It included information about respondents (such as age group, job title, organisation sector, their perceptions about BDIDM strengths and weaknesses, etc.) and their respective organisations (such as the type of IDM used and whether the organisation was aware of BDIM, etc.).

3.7.4. Data collection procedure

Researchers planned to identify participants using the search engine of a profession-based social network, namely LinkedIn. The use of other local IT-based bodies of professionals such as IITPSA (Institute of Information Technology Professionals South Africa) was equally considered. However, researchers opted for a uniform data collection process for all respondents. The LinkedIn platform was found more advantageous as it allowed a random search of the right participant. Randomness and respondents profiles were critical because of the sampling method adopted and sample frame.

Most of the potential participants were identified from the beginning of the research process, and others were added as the research evolved. The identification consisted of connecting with people suggested by the search result on LinkedIn. The search terms were based on the sample frame: job title, profile, location, etc. Requests for participation were regularly sent via LinkedIn direct messages to all the identified potential participants, 884 in total (15 to 20 participants at a time to allow for proper troubleshooting). The requests contained the link to the survey to accommodate participants who chose to participate. A pilot data collection was run for the 15 first participants to test the instrument before the actual data collection. However, this did not eliminate all human errors. For instance, the privacy variable was only measured on a binomial scale, unintentionally omitted from the interval scale variable list; hence was not part of the regression model nor Structural Equation Modelling.

3.8. Techniques and procedures of data analysis

This quantitative study opted for a statistical paradigm to analyse data. The statistical analysis was done using a combination of three software: (i) Microsoft Excel for some basic output, (ii) IBM statistical package for social science (SPSS) for most of the analysis, including Binary Logistic Regression modelling and Chi-Square tests, and (iii) IBM SPSS analysis of moment structures (AMOS) version 24.0 for confirmatory factor analysis. Since the research questions were both descriptive and explanatory, analysis techniques included both *descriptive* and *inferential statistics.*

Descriptive statistics enabled to give some background information necessary to understand the sample. Descriptive statistics also help to organise and summarise data and present it in a meaningful manner using tables, numbers, percentages, graphs, measures of central tendency (such as mean or average), and measures of variance (such as range and standard deviation, etc.) (Agresti & Finlay, 2009). These statistics further enabled the computation of the average perceptions to determine factors considered by security practitioners as strengths or weaknesses of blockchain and BDIDM adoption.

Inferential statistics often project statistics from a sample onto a targeted population. Inferential statistics includes analysing variance, correlations, and regression modelling, often leading to hypothesis testing. (Agresti & Finlay, 2009) Inferential statistics allowed the study to answer most of the research questions, including the primary one.

Inferential statistics often rely on probabilities to determine whether the variance observed in the dependant variable is due to the variance observed in independent variables rather than randomness (error). The confidence level for this study was set to 95%, with a subsequent margin of error of 5%. This margin of error determined the threshold alpha-value of .05 under which a null hypothesis was rejected: when the measured probability of randomness, p-value, was less than .05. The null hypothesises typically denied any significant relationship between the variables (Agresti & Finlay, 2009).

The primary analysis activities consisted of three main statistical tests: (i) Structural Equation Modelling (SEM) of the measurement model, known as confirmatory factor analysis (CFA), to test the model fitness; (ii) binary logistic regression modelling to test the study's hypotheses involving variables measured on interval scales, and (iii) Chi-Square tests of goodness of fit and association to test the study’s hypotheses involving variables measured on nominal scales. Other important analysis activities included reliability, validity, and normality testing as well as data cleaning.

3.8.1. SEM of the measurement model —CFA

SEM is a quantitative analysis framework that tests two principal models: the measurement model tested through confirmatory factor analysis and the structure model tested using path analysis (Blunch, 2012). Path model intends to investigate the hypothesised relationship between multiple dependent and independent variables, often including latent variables and covariances (Thakkar, 2020). Confirmatory factor model tests the relationship between observed measures or indicators and the latent variables or construct (Brown, 2015, p. 1).

In general, factor analysis is a common technique used to test data structure (model) and reduce ‘unnasty’ factors. Factor analysis can be either explorative or confirmatory (DeCoster, 1998). As their name suggests, exploratory factor analysis (EFA) explore data to propose a model that most fit it while confirmatory factor analysis (CFA) test the fitness of a predefined model to the data (Brown, 2015). CFA aims at measuring the instrument to see if “the hypothesized theoretical model is supported by the sample data” (Thakkar, 2020, p. 1). In a CFA, the model tested could have been previously explored using EFA or built based on a previously explored theory/ies in the literature (Marsh & Hocevar, 1985). CFA was suitable for this study since it had predefined the TOE-BDIDM model based on the TOE theory, in which the measuring instrument is rooted.

CFA is the “most commonly used in social research” (Ismael et al., 2021) and accommodates models involving latent variables like TOE-BDIDM. A latent variable is “an underlying characteristic that cannot be measured directly” (Vogt & Johnson, 2015, p. 226) but is hypothesised as an underlying group of observable variables. The TOE-BDIDM had latent variables at three levels. The lower level had security construct as a latent variable; the middle level had BDIDM_Char, BDIDM_Read, Infr_Comp, Org_Char Org_Read, Ind_Mark, Sup_Env, and Reg_Env constructs as latent variables; and the upper level had Technology, Organisation, and Environment constructs (as ‘latent of latent variables). These levels of latent variables in the TOE-BDIDM lead to a “higher-order CFA” (Brown, 2015, p. 287; Thakkar, 2020, p. 288) that was built and performed on data using the IBM SPSS Amos software.

The primary purpose of a CFA is to establish the “ability of a predefined factor model to fit an observed set of data”(DeCoster, 1998, p. 5). Table 6 describe the fitness indexes of the SEM measurement model and their respective level of acceptance. The acceptance level for the factor loading index, interpreted as the Standardized Regression Weight (symbolised by ʎ) (DeCoster, 1998), is often ʎ > 0.6 (Hair et al., 2006). In addition to testing the model fitness, CFA facilitates the assessment of reliability and validity of the measurements (Ahmad et al., 2016). The reliability and validity of measures are discussed in further sections.

Table 6. Fitness indexes for testing the appropriateness of BDIDM model in measuring the phenomenon

Name of category	**Name of index**	**Level of acceptance**	**Reference**
Absolute Fit	Discrepancy chi-square (Chisq)	p>.05	(Wheaton, 1987)
	Root Mean Square of Error Approximation (RMSEA)	RMSEA <.08	(Brown & Cudeck, 1993)
Incremental Fit	Goodness of Fit Index (GFI)	GFI >.90	(Jöreskog & Sörbom, 1984)
	Adjusted Goodness of Fit (AGFI)	AGFI >.90	(Tanaka & Huba, 1985)
	Comparative Fit Index (CFI)	CFI >.90	(Bentler, 1990)
	Tucker-Lewis Index (TLI)	TLI >.90	(Bentler & Bonett, 1980)
	Normed Fit Index (NFI)	NFI >.90	(Bollen, 1989)
Parsimonious Fit	Chi Square/Degree of freedom (Chisq/df)	Chisq/df <5.0	(Marsh & Hocevar, 1985)

3.8.2. Binary logistic regression modelling.

A binary logistic regression modelling “aims to see whether a value of the binary dependent variable can be predicted by the score of an independent variable” (Hinton et al., 2014, p. 319). For instance, in this study, the test sought to see if scores in the TOE factors could predict adopters and non-adopters of BDIDM to determine which factors might be the most significant predictors. In contrast to linear regression involved in the path analysis (Blunch, 2012), binary logistic regression

> *“is not based directly on the function of the straight line but on the logistic function, which ranges between 0 and 1. The point where a + bX= 0 is the point at which the prediction from 0 to 1 changes with a 1 (or yes value) predicted with positive values and a 0 (or a no value) predicted with negative values”.* (Hinton et al., 2014, p. 319)

In IBM Amos SPSS, the binary logistic regression test involves Omnibus test, Hosmer and Lemeshow’s goodness of fit, and Cox & Snell R Square (R^2)$_{to}$ estimate the explanatory strength of the latent variables. The significance of the regression depends on the significance of the Omnibus test ($p<.5$) and insignificance of the Hosmer and Lemeshow test ($p>.5$). The Omnibus test estimates the extent to which the proposed model is a better predictor than a basic model. Lemeshow’s goodness of fit test estimates the extent to which the proposed model differs from a perfect one (the one that accurately classifies responses according to their groups). Cox & Snell R$^{2 \text{ estimates}}$ how much of the variance observed in the dependent variable is due to the variances observed in the independent variables and how significant that is. Wald statistics also accompany the test to determine the significance of each component of the logistic regression. A classification table displays the number of observed cases the model predicted correctly and their percentages. (Hinton et al., 2014; Vogt & Johnson, 2015)

This study opted for binary logistic regression analysis over path analysis, mainly because of the binary nature of the dependant variable Adopt Indicator. Path analysis involves linear regression (Thrane, 2019) and requires that the dependant variable be measured on a ratio (Blunch, 2012) or interval scale (Vogt & Johnson, 2015). Hinton et al. suggest that a study is suitable for binary logistic modelling when it has “independent variables that are measured on an interval scale” and is “trying to predict group membership to a dependent variable measured on a nominal category” (2014, p. 319).

Independent variables part of the binary logistic modelling were the eight latent variables: BDIDM Characteristics, BDIDM Readiness, Infrastructure & Competencies, Networking and Structure, Organisation Readiness, Support Environment, Standards and Regulatory, and Industry and Market. These were indirectly measured on an interval scale. Their associated null hypotheses were H0$_{1,}$ H0$_{3,}$ H0$_4$, H0$_5$, H0$_6$, H0$_{8,}$ H0$_9$, and H0$_{10.}$ Since the Ninth independent variable, Organisation Size, as well as the item Blockchain Type, were nominal, they were tested separately using the Chi-Square test of goodness of fit and dependence. Their associated null hypotheses were H0$_2$ and H0$_{7.}$

3.8.3. Chi-Square tests

Chi-Square test of Goodness of fit compares expected and observed frequencies of the categories of a variable to assess whether there is a significant difference between them (Vogt & Johnson, 2015), while the Chi-Square test of association seeks to “compare two different sets of frequency counts to see if they are independent of each other" (Hinton et al., 2014, p. 13). These tests were appropriated to test $H0_2$ and $H0_{7,}$ stating that statistically, Blockchain Types or Organisation Sizes are equal and not associated with BDIDM adoption in organisations.

3.8.4. Reliability testing techniques and procedures

From a general perspective, "reliability refers to replication and Consistency" (Saunders et al., 2016, p. 202). It enquires whether the replication of earlier research design leads to the same findings in the later research. Other perspectives of reliability include "the extent to which data collection and analysis techniques and procedures "yield consistent findings" (Saunders et al., 2019). This is why some items were measured more than once to compare the consistency of the parallel responses.

From the quantitative analysis perspective, the reliability of scales can be tested in four ways: Test-Retest, internal consistency, Parallel forms, and Inter-Rater (Agresti & Finlay, 2009). Test-Retest estimates the stability of scores between two points of time (case of an experiment) using correlation. Internal consistency uses a well-known technique called Cronbach's Alpha to estimate the internal consistency of a group of items in measuring a construct. The Alpha coefficient ranges from .0 for no consistency to 1.0 for perfect consistency. Parallel forms reliability relies on correlation to estimate if different questions measuring the same thing lead to the same responses. Inter-Rater is concerned with the agreement between two responses on the same thing. (Vogt & Johnson, 2015). In this study, only internal consistency and parallel forms were applicable.

Another critical form of reliability used in the framework SEM is Construct Reliability (CR), also known as composite reliability. CR estimates the extends to which items represent the construct they intended to measure. CR is calculated using the formula $(\Sigma ʎ)^2 / [(\Sigma ʎ)^2 + (\Sigma 1 - ʎ^2)]$, where ʎ represents the factor loading of every item. (Ahmad et al., 2016) Table 7 below describe the level of acceptance of reliability and validity indexes.

Table 7. Reliability and validity indexes acceptance level (Level from which a the reliability and validity test will be considered statistically significant)

Name of category	Name of Index	Level of acceptance	Reference
Internal reliability	Cronbach Alpha	$\alpha \geq .5$	(Awang, 2015)
Construct reliability	Composite reliability	$CR \geq .6$	
Convergent Validity	Average Variance Extracted	$AVE \geq .5$	

3.8.5. Validity testing techniques and procedures

From a broader perspective, “validity refers to the appropriateness of the measures used, the accuracy of the analysis of the results and generalisability of the findings” (Saunders et al., 2016). Validity is concerned with “whether the findings are really about what they appear to be about”(Saunders et al., 2009, p. 157). In this study, multiple items were set to measure each construct to capture as many aspects of the constructs as possible.

The quantitative analysis assesses the validity of measures in termers of convergent, construct, and discriminant validity (Vogt & Johnson, 2015). Convergent validity is reached when all model items are statistically significant or the Average Variance Extracted (AVE) values of constructs are greater or equal to .5 (Blunch, 2012). AVE is calculated using the formula $\Sigma ʎ^2 / n$, where ʎ represents every item's factor loading and the number of items in the model (Ahmad et al., 2016). Construct validity is realised when fitness indexes, as shown in Table 7, “achieve the level of acceptance” (Ahmad et al., 2016, p. 3). Discriminant validity is achieved when there are no redundant items or constructs in the model, referred to as the absence of multicollinearity.

Multicollinearity refers to an ‘unintentional redundancy’ involving a group of variables highly correlated with other variable/s in opposite to collinearity that involves only two redundant variables. Redundant items tend to measure similar things hence are highly correlated. For instance, BDIDM type 1 and BDIDM type 2 are redundant items, a sort of collinearity intentionally set to verify the reliability of this particular data (parallel forms). Multi-collinearity is diagnosed when a tolerance value (the amount of variability in one independent variable that is not explained by the other independent variables) is less than .1 (Daoud, 2017). It can also be signalled by the Variance Inflation Factor (VIF) of an independent variable greater than 10 (Ahmad et al., 2016). To solve multicollinearity, Daoud suggests either “combining the highly correlated variables through principal component analysis” (p. 5) or omitting it from the analysis. Redundant constructs can be signalled by too high covariance between each pair of latent exogenous constructs, which should be less than .85. Other ways of diagnosing redundant constructs include verifying whether the square root of AVE for the construct is greater than the correlation between the corresponding constructs (Ahmad et al., 2016; Awang, 2015). This study only relied on assessing tolerance values and VIF to test multicollinearity.

3.8.6. Normality testing techniques and procedure

Normality testing estimates the degree to which data is symmetrically distributed around the mean to form a bell shape curve (Doane & Seward, 2011). Technically, it is about how a distribution follows the empirical rule. The empirical rule states that a normal distribution should have 68% of its data points falling within one standard deviation, 95% within two standard deviation, and 99.7% within three standard deviation from the mean (Wooditch et al., 2021).

Normality can be estimated based on the skewness and peakedness (known as Kurtosis) of data. Skewness test the shape and dispersion of data in the curve (Doane & Seward, 2011), while Kurtosis tests the curve's tallness or flatness (Cramer, 2003). A skewness or Kurtosis coefficient ranges from -1 to 1, and the skewness' sign reflects the skewness direction. Normality can also be assessed graphically (Wooditch et al., 2021), for instance, by visualising distribution in boxplots. Other normality tests include the Shapiro and Kolmogorov tests, relying on probability to reject the null hypothesis stating that a distribution is not normally distributed. However, these tests are difficult to pass for a sample size below 300 (Kim & Park, 2019). Therefore, this study only relied on boxplot visualisation, skewness, and Kurtosis coefficients to assess whether the distributions were approximately normally distributed.

3.8.7. Data cleaning techniques and procedure

Data were cleaned from abnormalities before the main analysis, dealing with outliers, erroneous or missing data. Regarding typing errors, inaccurate data were mitigated automatically by having the main survey questions all closed-ended. The survey was also set to auto-clean from missing data records: aborted responses for participants who chose to drop the questionnaire were not recorded. Except for nominal variables, the study had planned to replace outliers with the average value. This option seems more advantageous as it offered both the mitigation of unnecessary shrinking of the sample size that happens when records with outliers are excluded and a relatively acceptable boost of data normality so needed for a proper analysis. However, the study had planned to exclude any record that did not meet one of the study sample frame or ethical requirements.

3.9. Ethical considerations

This research did not cause any form of harm to participants. There was no need for respondents to reveal their identities nor the identity of their respective organisations. The survey was designed anonymously to preserve respondents' privacy. The research collected only necessary data, and no personal identifiable information was required. Participants were informed of the possible reuse of the data strictly for future research purposes.

Questionnaires were sent only after the ethics clearance process was completed and the university's approval was obtained (See Appendix 3). The cover page briefly explained the research purpose and allowed potential participants to either proceed with the questionnaire or drop it (See Appendix 1). Participants had the option to withdraw at any stage of the questionnaire. Due to the lack of funds, the participation was voluntary with no financial reward. It was assumed the research would indirectly benefit participants' organisations by raising awareness about the topic while inspiring.

3.10. Research high-level plan and execution

The research plan was subject to the academic calendar. Some deliverables were predefined by UCT's department of Information Systems, principally those related to research proposal and literature review. The rest were dependant on the individual plan of the researchers, as long as they were within the academic calendar. Table 8 below describe the main items and time frame that constituted the plan followed in executing this study.

Table 8. Plan followed in the execution of the research

ITEM	TIME FRAME/DEADLINE
Preliminary research proposal	From September to December 2019
Final research proposal	From March to April 2020
Participant identification	From the start till enough participants were identified
Research design presentation submission	7th August 2020
Writing up a final research design	From the last submission until the latest feedback (from the panel and supervisor) was applied.
Final research design submission	12th September 2020
Ethical form preparation	From September till 30th September
Compilation partial report	In conjunction with Ethical form preparation till final research design feedback applied
Ethical clearance submission	November 2020.

Data collection	Planned to start as soon as Ethics approval was granted received, from November 2020 to February 2021. But occurred from February to July 2021
Data analysis	Planed from March to May 2021 but took place from June to August 2021
Writing up findings and discussion	Planned for May but happened in September 2021
Compilation final report	Planned for June but happened in September to October 2021
Dissertation submission	Planned for August 2021 but happened end of October 2021
Safety margin	Two months periods were left unplanned to anticipate potential delays and were so used.

3.11. Research risk management

The researchers were aware of potential risks that could constraint the research process. Researchers had anticipated some of the most predictable risks while the unpredicted were dealt with as they were happening. Table 9 below describes procedures planned and adopted to mitigate some of the main risks, depending on their likelihood and impact.

Table 9. How the risks were managed to insurer the successful completion of the research in due time.

Risk	Impact	Likelihood	Mitigation procedure
Unresponsiveness of potential participants	Too few responses (< 300 valid responses) and delays in data collection	Was seen as very likely to happen and did happen, boosted by COVID-19.	The study was open to distributing questionnaires via other media like local IT-based bodies of professionals (e.g., IITPSA) but instead opted for consistency by extending the data collection time frame using the same media for all respondents.
Inconsistences in the data collection instrument	Invalid data collected or missing data	Was seen as very likely to happen and did happen	A pilot data collection was planned for the 15 first participants to test the instrument before the actual data collection. But there were still inconsistencies due to human error.
Delays in the ideal plan	Delays in dissertation submission	Was seen as likely to happen and did happen	Leverage safety margin by shifting time frame (reasonably extending the affected activity)
Research dropped due to lack or insufficient data	No dissertation submission	Was seen as less likely to happen but was on the edge of happening due to the COVID pandemic.	The researchers proactively monitored data collection and were open to changing the sample frame (e.g., considering all IT practitioners) and starting over if necessary. But this was significantly mitigated by the overall strategy of anticipated identification of many potential respondents.

Other unforeseen risks	Unknown serious impacts on the overall research process	Was seen as very unlikely to happen yet did happen due to the COVID-19 pandemic	Thanks to the earlier identification of potential respondents, the unusual low responsiveness rate was relatively mitigated by sending the survey to as many of them as possible (881 in total). The primary researcher managed to adapt to individual impacts, including those linked to the sudden shift to online learning and supervision: these could not be avoided.

3.12. Chapter summary

This chapter discussed the design and methodological framework followed in undertaking this research. The Saunders' Research Onion guided the framework to articulate methodological layers, from the research philosophy (the topmost layer) to techniques and procedures of data collection and analysis (the core part). The study chose subjectivism ontology and positivism epistemology as the study philosophy. The approach to the theory building was deductive. The study opted for a mono-method, only considering quantitative data collection and analysis methods. Survey was the research strategy, and the time horizon was cross-sectional. Techniques of data collection consisted of an online questionnaire rooted in the TOE theory. The study opted for a non-bias sampling method of probability sampling with simple random as a technique to identify potential respondents. Respondents were InfoSec practitioners in South African organisations. The latter constituted the research sample, chosen among a population made of every organisation globally. Data analysis techniques were principally made of SEM of measurement model known as CFA, binary logistic regression modelling, and the Chi-Square test of goodness of fit and association. The reliability and validity of measurements were to be assessed using a variety of techniques and procedures. The chapter ended by providing key ethical considerations and procedures followed to manage risks throughout the research process.

CHAPTER 4: ANALYSIS, FINDINGS, AND DISCUSSION

4.1. Introduction

The first section of this chapter reports the study's analysis and results. The results were obtained by performing a statistical analysis on quantitative data collected via an online survey rooted in the TOE theory, contextualized to BDIDM as shown in Figure 10. The analysis consisted of systematically applying the analysis plan as discussed in the design and methodology chapter in terms of techniques and procedures of data analysis. Alternative procedures were justified where the planned ones were not suitable.

The second section of this chapter discusses the implications of the findings, considering the research questions, objectives, and assumptions, attempting to understand the practical significance of the results by considering the literature review's perspectives. The second section highlights some unexpected findings of the analysis and additional observations about the theoretical framework involved.

4.2. Analysis and Findings

This section reports the research findings in the order in which the analysis was done. The results were obtained by performing a statistical analysis on quantitative data collected via an online survey based on the TOE-BDIDM model.

4.2.1. Analysis layout

The initial step involved data cleaning by first dealing with records beyond the study's sample frame and ethical requirements and then dealing with outliers in the dataset. The analysis then moved to perform some descriptive statistics necessary to understand the sample background. The background information included job title, the organisation size and sector, general categorical details (like the existence of IDM, awareness of BDIDM, blockchain type preferences, and BDIDM adoption), and perceptions about blockchain and BDIDM strengths as well as weaknesses. Next was reliability testing using Cronbach's Alpha technique to test internal consistency and correlation for parallel forms. Then followed confirmatory factor analysis to test the model fitness, composite reliability, convergent validity, construct validity, and discriminant validity. Next was normality testing using Skewness and Kurtosis tests to prepare data for the study hypothesis testing. The hypothesis followed and used binary logistic regression modelling for hypothesizes involving independent variables measured on interval scales and Chi-square test for hypotheses involving independent variables measured on nominal scales. The section ends with a summary of the hypothesis testing activity.

4.2.2. Data cleaning and sample size

The online survey recorded 115 responses out of 881 requests sent, indicating a participation rate of 13%. The survey was set to only record valid responses to anticipate the data cleaning. Thus, no missing data were found in the dataset. However, of the 115 valid responses, four were found beyond the study's sample frame or ethics requirements: two respondents were outside South African organisations, and the other two were younger than 18. As a result, the four responses were excluded from the analysis, leading to a sample size of 111. As shown in confirmatory factor analysis, the final model had 23 parameters (Excluding Conf, Int, and Avail items since they were combined into Security). This sample size is arguably acceptable given the overall good internal consistency and exceptional 'missing data level' of 0, even though it led to 4.8 responses per parameter over the requirement of five to ten responses per parameter (Kyriazos, 2018, p. 2223). Another key factor to consider about the sample size of this study is the unprecedented circumstances of the COVID-19 pandemic in which the study was undertaken impacted the participation rate more than anticipated. The next step in the data cleaning consisted in dealing with outliers.

The distributions were visualised in boxplots, as shown in Figure 11, to indicate the five extreme values: beyond the distribution ranges. The range is represented by the length of the boxplots, with the average value inside the boxes. Each box represents a distribution, with the *x* axe describing the variables' name associated with the distributions and the *y* axe indicating the five of the Likert scale used to measure the variables (1 for 'Strongly disagree' to 5 for 'Strongly agree'). The small circles indicate the outliers with the corresponding y as their values. The numbers surrounding the circles indicate the location of outliers in the dataset (record IDs). Responses with outliers were not deleted to avoid unnecessary shrink of the sample size. Except for nominal (categorical) variables, all outliers were replaced by the average values of the respective distributions. Categorical variables were not concerned by outliers replacement to avoid erroneous data: categorical data tend to be nominal, making their average meaningless.

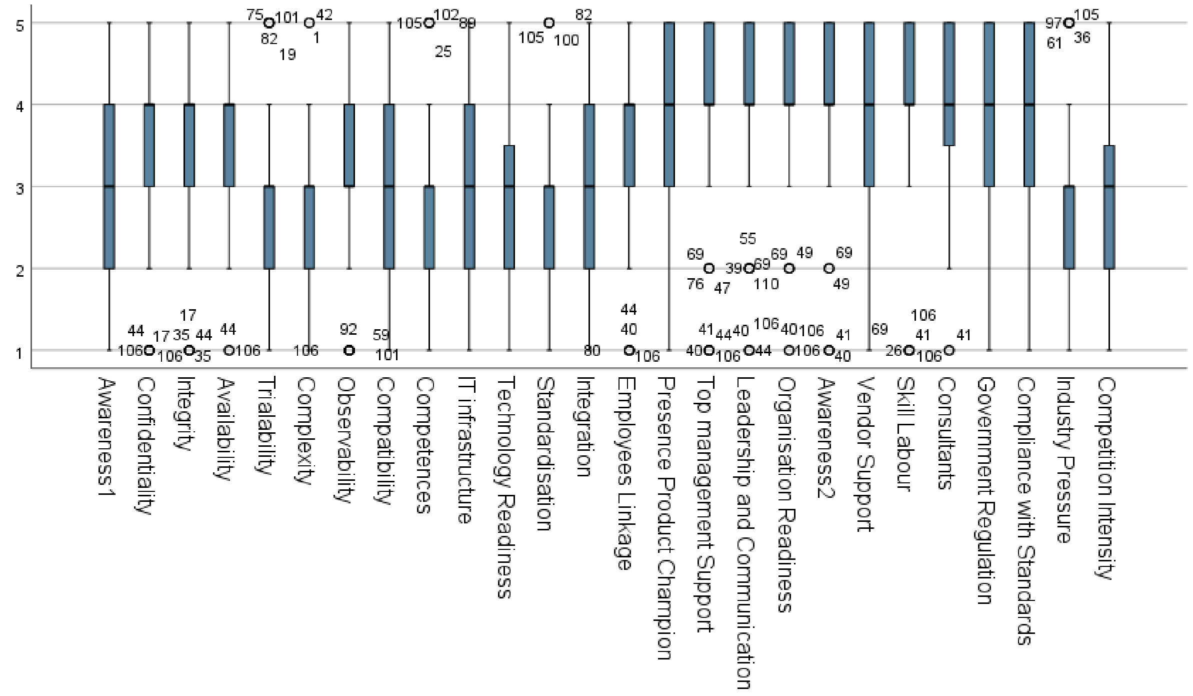


Figure 11. Visualising outliers in the dataset using boxplots technique. The small circles indicate the outliers: the number beside the circle indicating the outlier location (line number/record) in the dataset and the corresponding y indicate the outlier values).

4.2.3. Background information

The 111 respondents who constituted the sample were InfoSec practitioners with various job titles, as shown in Table 10. Nearly the entire sample's job titles aligned with the sample frame, previously discussed in the research design as managerial levels of InfoSec: 14 officers, 16 managers, and 78 technical staff. An additional level, made of two security executives, was not anticipated but aligned with the sample frame. Respondents could enter their job titles when they could not pick one representative from the list provided.

The table also shows that all the four organisations sizes were represented in the sample. The organisation's sizes were determined by the number of employees as estimated by each respondent: above 250 employees for large enterprises, 51 to 250 employees for medium Enterprises, 11 to 50 employees for small enterprises, and below ten employees for micro-enterprises. Of the 111 respondents, 70 belonged to large enterprises the rest 41 to SMEs (22 to medium enterprises, 13 to small enterprises, and the rest to micro-enterprises).

Table 10. Description of the sample from the managerial levels perspective

Descriptive statistics

InfoSec managerial level				**Organisation Size**			
Title	**Freq.**	**Freq. level**	**Percent level**	**Micro**	**Small**	**Medium**	**Large**
Executive:		3	2.70	0	1	0	2
Information or Cyber Security Governance/Executive	3						
Officer:		14	12.61	2	3	1	8
IAM Officer	7						
Chief Information Security Officer	3						
Chief Information Officer	2						
Chief Technology Officer	2						
Manager:		16	14.41	1	1	1	13
InfoSec Manager	11						
InfoSec Architecture Manager	1						
Network Security Manager	1						
Data Centre Manager	1						
Operation Manager	1						
Project Manager	1						
Technical Staff:		78	70.27	3	8	20	47
Information and/or Cyber Security Administrator/Analyst/Specialist/Architect/Consultant	40						
IAM Administrator/Analyst/Specialist/Consultant/Engineer	9						
Network Security Administrator	5						
IT auditor/Program Analyst/Program Analyst	3						
Cloud Administrator/Engineer/Consultant	4						
System Administrator/Engineer	4						
Software Developer/Engineer	2						
Solutions Architect	4						
Data Engineer	2						
PenTester, ERP Analyst, Technical Support, technical engineer	5						
Total	111	111	100.00	6	13	22	70
Total				111			

The pie chart in Figure 12 describes organisation sectors represented in the sample according to the Statistics South Africa department classification (stats-sa, inedi). Most respondents' organisation fell under information and communication technology (47 respondents', accounting for 42 % of the sample) or financial & Insurance (30 respondents, accounting for 27 % of the sample) sectors.

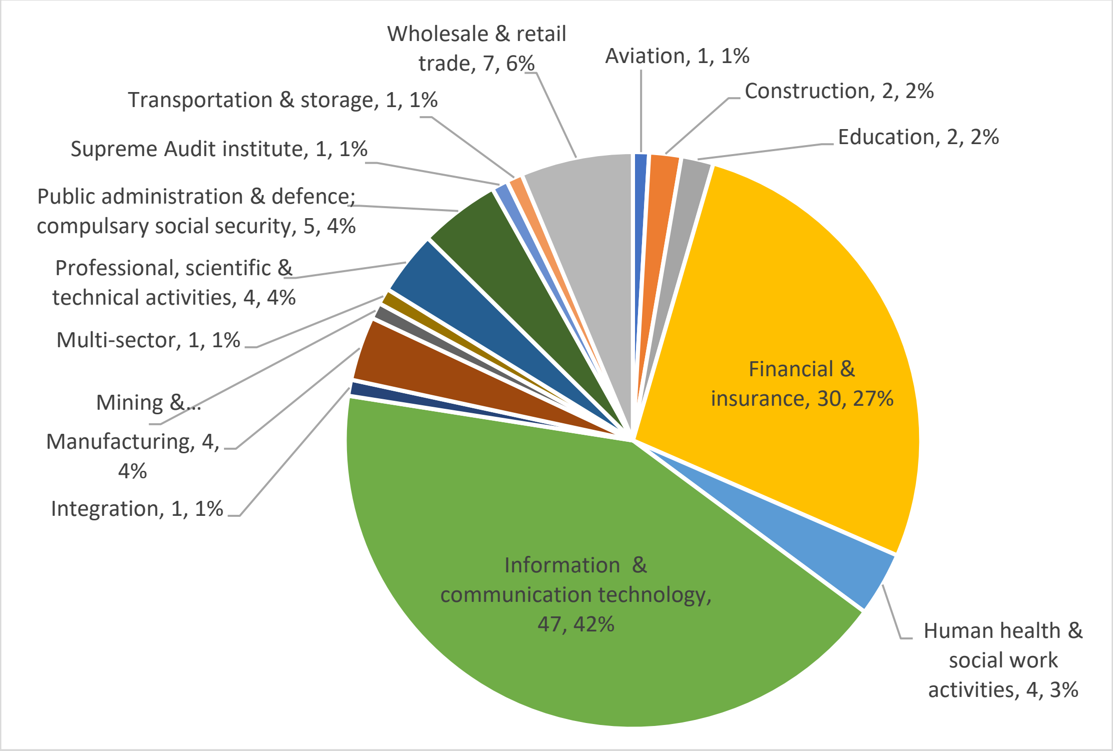


Figure 12. Description of the sample from the organisation sectors perspective

Table 11 gives additional background information about IDM system existence, awareness of BDIDM, blockchain type, and the intention to adopt BDIDM. When asked about the IDM model used, three respondents indicated their organisation combined BBIDM with ID-as-a-service and federated IDM. Sixteen indicated they were combining centralised IDM with other distributed IDM but non-blockchain-based. The rest used one or a combination of different centralised IDM models.

Elsewhere, a list of key factors promoting and constraining the adoption (as discussed in the literature, see Table 3 and 4) was randomly proposed to respondents to choose which they perceived as ‘strengths’ or ‘weaknesses’ of blockchain and BDIDM adoption. These items were measured on a binary scale: the strength value was quantified to 1, and the weakness values quantified to 2. Table 12 reports the average values of the observed responses and their standards deviation. A value close to 1 indicates the associated factor was perceived as a strength and a value close to 2 indicates it was perceived as a weakness.

Table 11: Additional demographic information sample additional information

Descriptive statistics

	Frequency	Percent
Age group		
Between 18 and 40	82	71.0
Over 40	31	27.0
Does your organisation have an established IDM system?		
I don’t know	3	2.7
No	8	7.2
Yes	100	90.1
Total	111	100.0
Is your organisation aware of BDIDM?		
No	40	36.0
Not sure	18	16.2
Yes	53	47.7
Total	111	100.0
Which type of blockchain do you think is suitable for your organisation?		
Public permissionless blockchain	10	9.0
Public permissioned blockchain	27	24.3
Private permissioned blockchain	74	66.7
Total	111	100.0
Would you recommend BDIDM to your organisation?		
Yes	80	72.1
No	31	27.9
Total	111	100.0

Table 12. Perceptions about BDIDM adoption enablers and barriers (factors promoting or constraining blockchain adoption).

Descriptive Statistics

	Mean	Std. Deviation
Integrity, Authentication, & Trust	1.07	.255
Security	1.09	.286
Scalability and Performance	1.10	.300
Programmability & Automation	1.16	.367
User Privacy	1.17	.376
Transparency & Auditability	1.19	.393
Immutability & Verifiability	1.19	.393
Decentralisation & Disintermediation	1.25	.434
Controllability /Monitoring	1.25	.434
Interoperability of ID	1.28	.450
Vendor support and Sustainability	1.42	.495
Culture & Adaptation	1.64	.481
Cost of Implementation	1.71	.455
Uncertain Regulatory Status /Lack of Standards	1.80	.400
Skill Availability	1.87	.337
Reluctance to change	1.87	.337

4.2.4. Assessing internal reliability: Cronbach's Alpha

In Table 13, the Alpha coefficient for all constructs (including the sub-construct of Security) indicated a good consistency, except for Organisation Readiness. This result means a good percentage of the variance observed in the constructs; respectively, 78% for Security, 72% for BDIDM Characteristics, 65% for BDIDM Readiness, 69% for IT Infrastructure and Competences, 78% for Organisation Characteristics 78% for Support Environment, 89% for Industry and Market Environment, and 78% for Regulatory Environment; is accurate and reliable. The residual variance observed in the constructs, that is respectively 22% for Security, 28% for BDIDM Characteristics, 35% for BDIDM Readiness, 31% for IT Infrastructure and Competences, 22% for Organisation Characteristics 22% for Support Environment, 11% for Industry and Market Environment, and 22% for Regulatory Environment; is due to randomness.

It is important to note that this test only considered variables measured on an interval scale as they were involved in the main analysis. Security variable that was part of the BDIDM Characteristics construct was computed as the average of its constituents, i.e., Confidentiality, Integrity, and Availability, just as predesigned according to the theory of CIA triad previously discussed in the literature.

Table 13. Alpha coefficient per construct.

Reliability Statistics

	Cronbach's Alpha	N of Items
Security	.78	3
BDIDM Characteristics	.72	6
BDIDM Readiness	.65	2
IT Infrastructure and Competences	.69	2
Organisation Characteristics	.78	4
Organisation Readiness	.45	2
Support Environment	.78	3
Industry and Market Environment	.89	2
Regulatory Environment	.78	2

Table 14 lists the items that were involved in the Cronbach's Alpha test for each construct. The two last columns respectively show the correlation coefficient of each item with the rest of the items in the construct and how the Alpha coefficient would either increase or decrease if that related item was deleted. Thus, Awareness1 was excluded from Organisation Characteristics construct to improve its alpha coefficient to .83 from the initial .45. However, before excluding this problematic variable, the test of the parallel form was performed to assess any possibility of combining it with Awareness2.

Table 14. Items involved in Cronbach's Alpha test per construct.

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Security				
Confidentiality	7.63	2.02	.55	.76
Integrity	7.45	1.78	.75	.55
Availability	7.55	1.96	.55	.77
BDIDM Characteristics:				
Security	14.70	9.04	.30	.72
Trialability	15.62	7.82	.51	.66
Observability	15.14	8.37	.37	.70
Compatibility	15.53	7.16	.54	.65
Complexity	15.73	7.48	.55	.65
Integration	15.62	7.06	.45	.69
BDIDM Readiness:				
Standardisation	2.72	1.17	.48	.
Technology Readiness	2.61	.91	.48	.
IT Infrastructure and Competences:				
IT infrastructure	2.49	1.02	.53	.
Competences	2.76	1.22	.53	.
Organisation Characteristics:				
Employees Linkage	12.52	3.88	.47	.78
Presence Product Champion	12.46	2.97	.59	.74
Top management Support	12.04	3.29	.72	.66
Leadership and Communication	12.11	3.62	.61	.72
Organisation Readiness:				
Organisation financial Readiness	7.41	2.02	.48	.10
Awareness1	8.65	1.60	.12	.83
Awareness2	7.40	2.17	.38	.24
Support Environment:				
Vendor Support	8.46	1.70	.53	.791
Skill Labour	8.32	1.47	.66	.649
Consultants	8.49	1.50	.66	.654
Industry and Market:				
Industry Pressure	2.63	.94	.80	-
Competition Intensity	2.55	.79	.80	-
Regulatory Environment:				
Government Regulation	3.98	.84	.56	-
Compliance with Standards	3.69	1.12	.56	-

4.2.5. Assessing parallel forms

The study had several questions measuring the same variables, often using different scales (nominal on one occasion and interval on the other) and sometimes using the same scale, creating a sort of parallel variables. Among those using the same scales, two pairs were used to measure the type of blockchain for the enterprise perspective and organisation awareness about BDIDM. The parallel form test estimated the correlation coefficients between the pairs of responses using Spearman's correlation for nominal variables and Pearson correlation for intervals.

The blockchain type pairs consisted of Blockchain Type1 and Blockchain Type2 variables. Initially, all respondents were asked to choose from a list of three types of blockchain, accompanied by a short description, which they perceived the most suitable for their organisation. That formed the Blockchain Type1 variable. Toward the end, respondents were virtually split into two groups: adopters and non-adopters. The exact list of blockchain types was proposed for adopters to choose which they would be likely to recommend to their organisation, for non-adopters which they would recommend to their organisation if they were required to. The two group responses were reunified to form the Blockchain Type 2 variable. Table 15 shows that the correlation between responses in Blockchain type 1 and Blockchain Type 2 variables is statistically very significant as the p-value is far less than .5. Therefore, the observation made about Blockchain type for organisations in this study is accurate and reliable.

But the study did not combine the two variables due to their nominal nature: their average is meaningless. Blockchain Type 2 was chosen over Blockchain Type 1 for the rest of the analysis because it was more reliable. A separate Cronbach’s Alpha test for BDIDM Characteristics construct including these categorical variables suggested that Blockchain Type 2 would decrease BDIDM Characteristics’ internal consistency to 63% if deleted compared to Blockchain Type 1 increasing it to 66%.

Table 15. Parallel forms test between Blockchain Type1 and Blockchain Type 2

Correlations

			Blockchain Type1
Spearman's rho	Blockchain Type2	Correlation Coefficient	.653**
		Sig. (2-tailed)	.000
		N	111

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

Table 16. Parallel forms test between Awareness1 and Awareness2

Correlations

		Awareness1	Awareness2
Awareness1	Pearson Correlation	1	
	Sig. (2-tailed)		
	N	111	
Awareness2	Pearson Correlation	.064	1
	Sig. (2-tailed)	.508	
	N	111	111

Awareness was measured on three occasions in the survey, one using a nominal scale and the rest using a Linkert scale of five values. On the first, respondents were required to answer with a "Yes", "Not Sure", or "No" to whether their organisation were aware of BDIDM (Awareness0, as described in the background information section). On the second occasion, respondents were asked to rate the extent to which they agreed or disagreed with whether their respective organisation was aware of BDIDM (Awareness1). On the last occasion, respondents were asked to rate the extent to which they agreed or disagreed with whether awareness about BDIDM was necessary to its adoption in their respective organisation (Awareness2). Since Table 16 shows a p-value of more than .05, the hypothesised correlation between Awareness1 and Awareness2 was proven statistically insignificant. The survey questions might not have been semantically identical enough and resulted in measuring distinct aspects of awareness. Thus, Awareness1 and Awareness2 could not be combined. Awareness2 was chosen over Awareness1 because it was far more reliable. Cronbach's Alpha test already suggested the exclusion of Awareness1 from the Organisation Readiness construct to improve its internal consistency.

4.2.6. SEM of the measurement model: Confirmatory factor analysis

The second-order CFA shown in Figure 13 represents the SEM measurement model of TOE-BDIDM performed on data using IBM Amos SPSS. Directional arrows indicate causal relationships, bidirectional arrows indicate the covariance relationships, and circles measure error on each 'caused' variable. The concept of error is a SEM principle suggesting that no measurement is perfect. There is always some randomness accompanying it that should be isolated from the true score for accurate results. Hence the equation *Variable = True_Score +*

Error (Blunch, 2012). Numbers on directional arrows indicate the factor loadings of items on constructs while those on bidirectional arrows covariance rate between constructs. Rectangles on the left-hand side represent indicators items (also referred to as indicators). Ovals in the middle represent first-order constructs. Ovals on the right-hand side represent second-order constructs. The First-order construct moderate the relationship between the indicators and second-order constructs. The Second-order construct will moderate the relationship with the dependant variable of Adopt Indicator. Tables 17 to 20 report the model fitness indexes for both the hypotheses and the modified model, respectively, as shown in Figures 13 and 14.

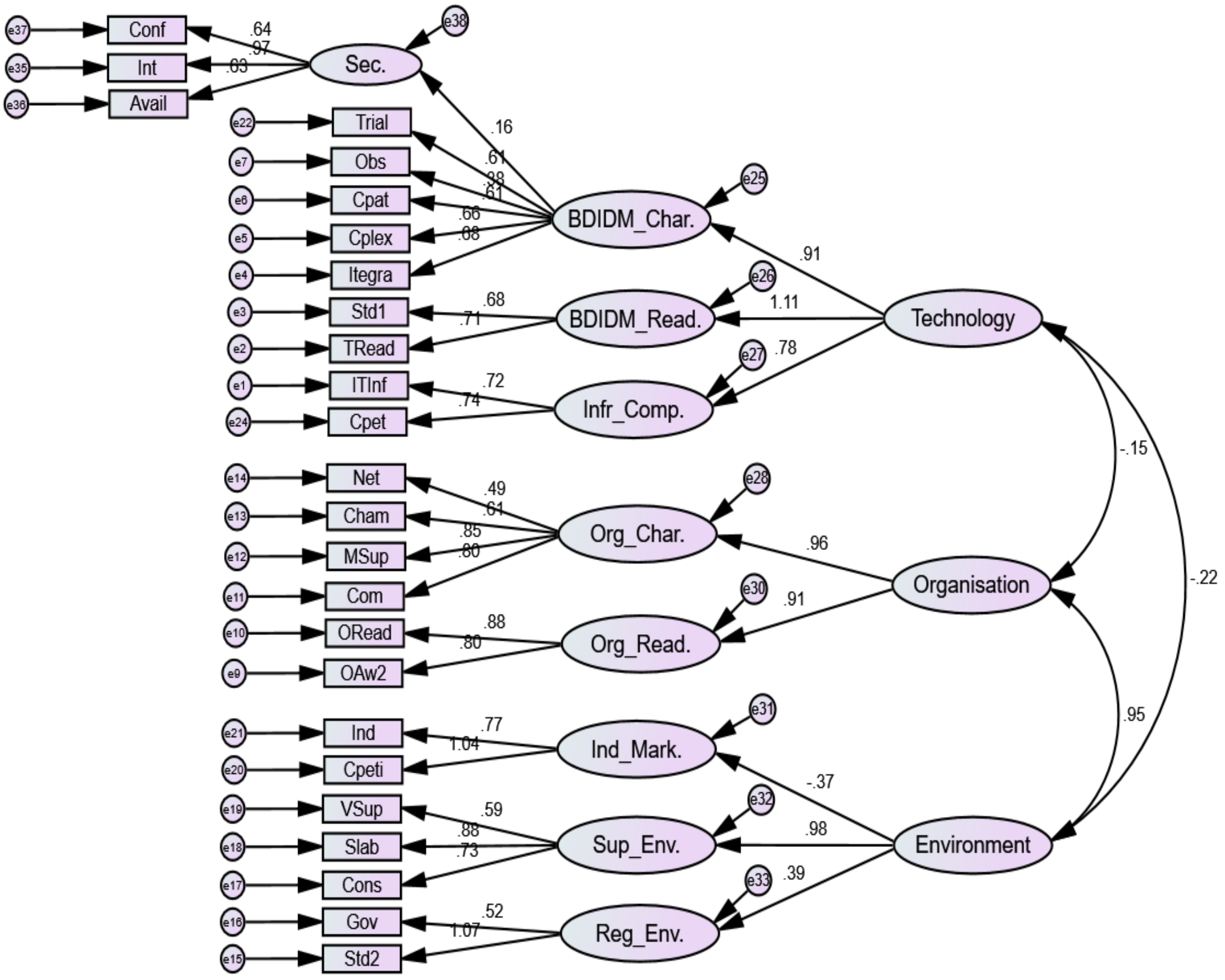


Figure 13. Higher-order Confirmatory Factor Analysis of the hypothesised TOE-BDIDM model

Table 17. Discrepancy chi-square (Chisq)

	Hypothesised TOE- BDIDM					Modified TOE- BDIDM model				
Model	NPAR	CMIN	DF	P	CMIN/DF	NPAR	CMIN	DF	P	CMIN/DF
Default model	62	459.501	263	.000	1.747	57	172.438	153	.135	1.127
Saturated model	325	.000	0			210	.000	0		

	Hypothesised TOE- BDIDM					Modified TOE- BDIDM model				
Model	NPAR	CMIN	DF	P	CMIN/DF	NPAR	CMIN	DF	P	CMIN/DF
Independence model	25	1550.363	300	.000	5.168	20	1206.522	190	.000	6.350

Table 18. Goodness of Fit Index (GFI)

	Hypothesised TOE- BDIDM model				Modified TOE- BDIDM model			
Model	RMR	GFI	AGFI	PGFI	RMR	GFI	AGFI	PGFI
Default model	.118	.769	.714	.622	.053	.868	.819	.632
Saturated model	.000	1.000			.000	1.000		
Independence model	.207	.320	.263	.295	.234	.329	.258	.298

Table 19. Baseline Comparisons

	Hypothesised TOE- BDIDM model					Modified TOE- BDIDM model				
Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	.704	.662	.847	.821	.843	.857	.823	.982	.976	.981
Saturated model	1.000		1.000		1.000	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000

Table 20. Root Mean Square of Error Approximation (RMSEA)

	Hypothesised TOE- BDIDM model				Modified TOE- BDIDM model			
Model	RMSEA	LO 90	HI 90	PCLOSE	RMSEA	LO 90	HI 90	PCLOSE
Default model	.082	.070	.095	.000	.034	.000	.058	.852
Independence model	.195	.185	.204	.000	.221	.209	.233	.000

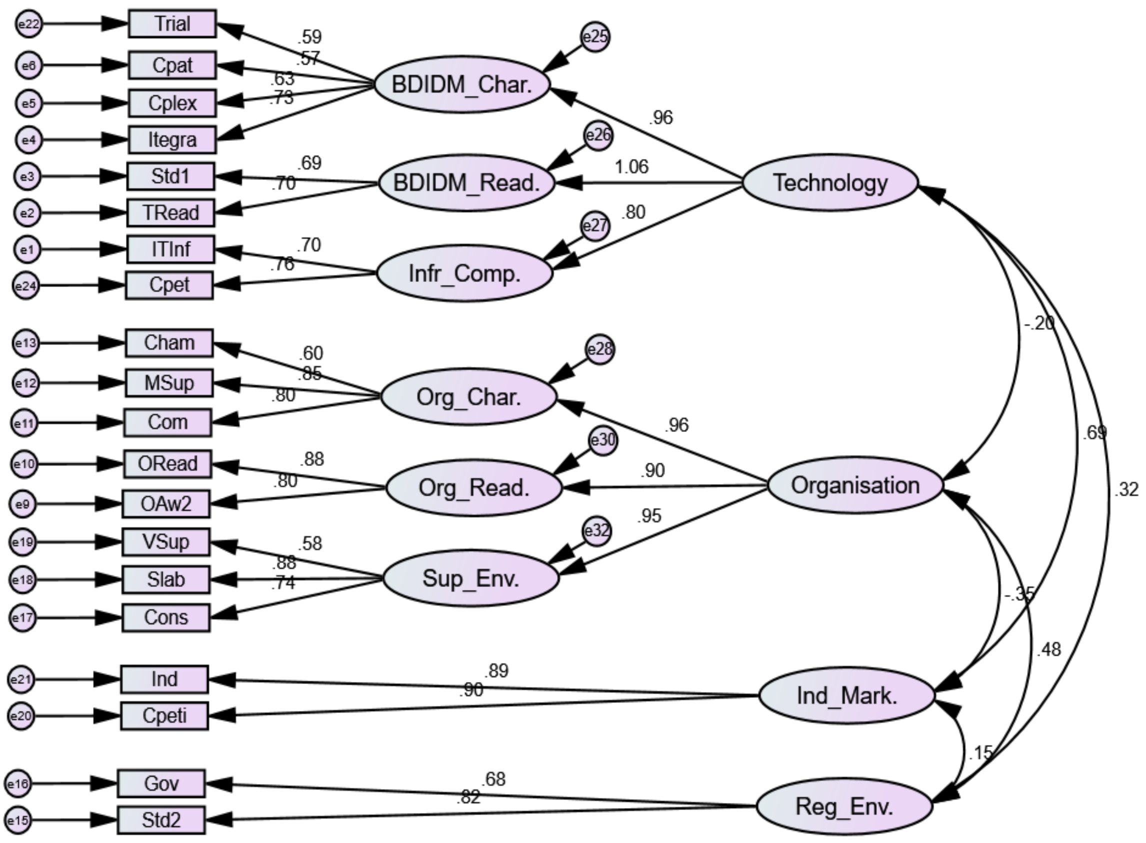


Figure 14. Higher-order Confirmatory Factor Analysis of the Modified TOE-BDIDM model

a) *Assessing the model fitness*

Fitness indexes for the hypothesised model displayed p =.0, absolutely less than.05, and Chisq/df =263, far more than the threshold of 5.0, in Table 17. GFI and AGIF in table 18, and CFI, TLI and NFI in Table 19 are all less than .90 and RMSEA in Table 20 is less than .80. Therefore, the hypothesised model shown in Figure 13 is a poor fit for this data.

The model was modified to improve the fit, as shown in Figure 14. The modification to better factors with relatively acceptable construct as most of the factor loadings were then at least above .5. The first improvement was to reduce the number of indicators per latent variable, excluding those with a poor factor loading of ʎ<.5. In this way, Sec, Obs, and Net were excluded from the model. The second improvement was to add some covariances between errors, only for those belonging to the same construct, as suggested by improvement indices of the test. The third improvement and major modification was to solve the suspicious 'redundancy' signalled by a very high covariance of .95 between Technology and Environment constructs. The procedure followed to solve this issue is discussed later in the discriminant validity section. Table 21 summarises the fitness indexes assessment for both the hypothesised and the modified model.

Table 21: Results summary of fitness indexes testing the appropriateness of TOE-BDIDM

Name of category	Level of acceptance	Hypnotized model	Modified model
Absolute Fit	p>.05	Not achieved	Achieved
	RMSEA <.08	Not achieved	Achieved
Incremental Fit	GFI >.90	Not achieved	Not achieved
	AGFI >.90	Not achieved	Not achieved
	CFI >.90	Not achieved	Achieved
	TLI >.90	Not achieved	Achieved
	NFI >.90	Not achieved	Achieved
Parsimonious Fit	Chisq/df (CMIN/DF) <5.0	Achieved	Achieved

In addition to fitness, the higher-order CFA also facilitated the assessment of construct reliability, convergent validity, construct validity, and discriminant validity.

b) *Assessing construct reliability*

Table 22 reports good construct reliability of the hypothesised model as nearly all the CR values for both first and second-order constructs were greater than .6, except for the

Technology construct that was entirely below this threshold. This result means an overall good proportion variance is shared between indicators and the constructs they intended to measure.

c) *Assessing convergent validity*

Of the nine first-order constructs, Table 22 shows that eight did more or less meet the acceptable level of convergent validity as their AVE values are greater than .50, even as BDIDM_Read and Org-Char's are just about that threshold with BDIDM_Char' s remarkably low. After excluding poorly loading factors, the modified model reported AVE values of .39 for BDIDM_Char, .49 for BDIDM_Read, and 56 for Org-Char. Since BDIDM-Char's AVE value did not improve, Sec and Obs items were reconsidered in the binary logistic modelling. This choice was also motivated by BDIDM_Char's excellent internal consistency of α = .72 and good construct reliability of CR = 68 in the hypothesised model.

Of the three second-order constructs, only the Environment's AVE value met the threshold of greater than .6. The modification done on the model did not improve this result, as the Technology and Organisation's AVEs were still below .6, respectively moving from .11 to .12 and from .13 to 12. However, the 'P' column of Table 23 indicates that regression weights of about the entire hypothesised model are statistically significant. Therefore, the convergent validity of the hypothesised model is arguably acceptable. In other words, the variation in the constructs is reasonably explained by their respective item constituent.

d) *Assessing construct validity*

Construct validity is realised when "fitness indexes achieve the level of acceptance" (Ahmad et al., 2016, p. 3). The hypothesised model did not meet this requirement since the CFA suggested that it did not perfectly fit the data. The modified model offered a better fit.

e) *Assessing discriminant validity*

The collinearity performed earlier using linear regression analysis in SPSS, reported in the column Table 23 suggested no case of multi-collinearity. Column "Tol" shows that all items and construct's tolerance values were greater than .1, and column "VIF" shows that their respective VIF values were less than 10. Therefore, the items and first-order constructs of the hypothesised model were distinctive, fulfilling the requirement of discriminant validity.

However, the CFA of the hypothesised model done in IBM Amos SPSS, as shown in Figure 13, did indicate a possible redundant second-level construct. The presumed redundancy was signalled by a remarkably high covariance of .95 between the Technology and Environment constructs. The Environment construct appeared more problematic because only one of its constituents, Sup_Env, was strongly loaded with ʎ = .98. The rest were unusually weak, Ind-Mark with ʎ = .37 and Reg-Env with ʎ = .39. This divergence meant three constituents did not share a fair portion of variance with the Environment construct they intended to measure. Unexpectedly, Sup_Env was also strongly loading on the Organisation with ʎ = .95, causing it to be redundant with Environment. The problem was solved by moving Sup_Env into the Organisation and isolating the remaining variables.

Nevertheless, this change did not affect further binary logistic regression analysis since it only involved the first-order constructs. Daoud (2017)'s suggestion in solving redundancy of either "combining the highly correlated variables through principal component analysis, or omitting a variable from the analysis that associated with another variable (s) highly" (p. 5) was not applicable. The 'multicollinearity' happened at the higher level of the model, making it unreasonable to combine or omit such constructs.

Table 22. Results summary of reliability and validity indexes of the hypothesised model

Item				**First-order Construct**							**Second-order Construct**		
Name	*Tol.*	*VIF*	*ʎ*	*Name*	*CR*	*AVE*	*α*	*VIF*	*Tol.*	*ʎ*	*Name*	*CR*	*AVE*
Conf	.41	2.43	.64	Sec	.80	.58	.78				Technology	.75	.11
Int	.32	3.09	.97										
Avail	.45	2.24	.63										
Sec			.16	BDIDM_Char	.68	.29	.72	.46	2.17	.91			
Obs	.51	1.96	.38										
Itegra	.36	2.76	.73										
Cplex	.48	2.10	.61										
Cpat	.41	2.43	.56										
Trial	.55	1.82	.58										
Std1	.42	2.37	.66	BDIDM_Read	.65	.49	.65	.38	2.64	1.11			
TRead	.39	2.54	.73										
ITInf	.39	2.55	.66	Infr_Comp	.69	.53	.69	.59	1.72	.78			
Cpet	.44	2.27	.79										
Net	.44	2.18	.49	Org_Char	.78	.48	.78	.42	2.40	.96	Organisation	.65	.13
Cham	.44	2.29	.57										
Com	.33	3.05	.79										
MSup	.26	3.92	.85										
ORead	.28	3.57	.86	Org_Read	.82	.70	.83	.42	2.40	.91			

OAw2	.39	2.59	.80										
Cons	.39	2.58	.73	Sup_Env	.78	.55	.78	.59	1.71	.98	Environment	.45	.58
Slab	.28	3.62	.89										
VSup	.57	1.74	.58										
Std2	.45	2.22	.83	Reg_Env	.72	.57	.78	.39	2.57	0.39			
Gov	.46	2.19	.67										
Ind	.25	4.01	.88	Ind_Mark	.79	.80	.89	.59	1.71	-0.37			
Cpeti	.22	4.50	.91										

Table 23. Regression Weights

			Estimate	S.E.	C.R.	P
BDIDM_Char.	←	Technology	.765	.137	5.590	***
BDIDM_Read.	←	Technology	1.000			
Infr_Comp.	←	Technology	.687	.128	5.378	***
Org_Char.	←	Organisation	1.000			
Org_Read.	←	Organisation	.918	.101	9.105	***
Ind_Mark.	←	Environment	-.588	.153	-3.852	***
Reg_Env.	←	Environment	.611	.144	4.256	***
Sup_Env.	←	Environment	1.000			
Sec.	←	BDIDM_Char.	.167	.112	1.494	.135
ORead	←	Org_Read.	1.000			
Net	←	Org_Char.	.559	.107	5.208	***
Cham	←	Org_Char.	.921	.134	6.858	***
Itegra	←	BDIDM_Char.	1.000			
Cplex	←	BDIDM_Char.	.771	.130	5.947	***
Cpat	←	BDIDM_Char.	.780	.142	5.492	***
Stdv1	←	BDIDM_Read.	.843	.127	6.659	***
TRead	←	BDIDM_Read.	1.000			
ITInf	←	Infr_Comp.	1.056	.187	5.661	***
Cpet	←	Infr_Comp.	1.000			
Std2	←	Reg_Env.	1.000			
Gov	←	Reg_Env.	.562	.233	2.412	.016
Cons	←	Sup_Env.	.818	.093	8.803	***
Slab	←	Sup_Env.	1.000			
Ind	←	Ind_Mark.	.681	.146	4.672	***
Cpeti	←	Ind_Mark.	1.000			
VSup	←	Sup_Env.	.646	.098	6.569	***
Trial	←	BDIDM_Char.	.674	.122	5.546	***
OAw2	←	Org_Read.	.906	.095	9.572	***
Conf	←	Sec.	.687	.124	5.562	***
Int	←	Sec.	1.000			
Avail	←	Sec.	.703	.128	5.508	***
Obs	←	BDIDM_Char.	.413	.117	3.531	***
MSup	←	Org_Char.	1.000			
Com	←	Org_Char.	.904	.092	9.860	***

The next step of the SEM framework after a CFA is often to test the structure model of the modified model via path analysis. This was neither suitable nor feasible in this study for the reasons previously mentioned in the research design and methodology chapter. Instead, the study opted for binary logistic regression analysis. But since any regression analysis requires data to be normally distributed, it was necessary to test the normality of the distributions involved before performing the test.

4.1.1. Normality testing

A normal distribution should have skewness and kurtosis very close to 0. A common rule on skewness and Kurtosis assessment suggest that the statistic's ratio on the test's standard error should be less than the Z-distribution's critical value of 1.96 (Doane & Seward, 2011). Another rule adds that the skewness statistic should be less than .8 (Trafimow et al., 2019). Table 24 shows that only Org_Read and Reg_Env had some skewness issues as their skewness critical value were greater than 1.96. But their skewness, and Kurtosis statistics were mostly less .8. Therefore, it was concluded that the eight distributions were approximately normally distributed and fit for further analysis.

Table 24: Skewness and peakiness of distributions

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
BDIDM_Char	111	1.81	4.50	3.0783	.54416	-.289	.229	.096	.455
BDIDM_Read	111	1.00	4.50	2.6629	.87545	-.075	.229	-.910	.455
Inf_Comp	111	1.00	4.00	2.6238	.92610	-.275	.229	-.892	.455
Org_Char	111	3.00	5.00	4.0945	.59703	-.349	.229	-.808	.455
Org_Read	111	3.00	5.00	4.3244	.63175	-.640	.229	-.416	.455
Indu_Mark	111	1.00	4.00	2.5887	.87946	-.201	.229	-.728	.455
Sup_Env	111	3.00	5.00	4.2112	.59220	-.391	.229	-.591	.455
Reg_Env	111	1.00	5.00	3.8378	.87168	-.536	.229	.558	.455

4.1.2. Binary logistic regression analysis

Binary logistics regression analysis considered the hypothesis model over the modified since the were no redundant items or redundant first-order construct. The overall reliability and validity were reasonable, with excellent internal consistency for most first-order constructs. Moreover, the study's hypotheses concerned the direct relationship between the first-order constructs (latent variables) and the dependant variable, without necessitating any moderators by second-order constructs of Technology, Organisation, and Environment. The latent variables were computed as the average of their respective indicators. By the way, the modified model could not be tested using binary logistic modelling, which is bivariate and does not allow multiple regressions nor covariances in the model. Most importantly, as previously discussed in the research design and methodology chapter, binary logistics regression was more suitable than path analysis due to the binary nature of the dependant variable, adopt indicator.

The binary logistic regression analysis was performed using IBM Amos SPSS and utilised the ‘Enter’ method. The enter method means the factors were simultaneously inserted together in the regression model at Step 1 to see their overall interaction. No factor was delayed or privileged over others. The results are reported in tables 27 to 31.

Table 25 shows a significant Omnibus result of $\chi^2 = 31.15$, DF = 8, p =.0 while Table 27 shows an insignificant Hosmer result of $\chi^2 = 8.48$, df = 8, p = .39. These results indicate that the binary logistic regression is significant. The variance observed in the Adopt Indicator dependent variable is due to the variance observed in the TOE factors (the eight latent variables) rather than randomness. Table 26 reports Cox & Snell R^2 of .245 to .351. Since the study’s confidence level is 95%, this interval means that if the data collection were repeated 20 times, 19 would have 24.5 to 35.1% of the variance observed in the Adopt Indicator due to the variance in the TOE factors. Therefore, there is a relationship between the TOE factors and BDIDM adoption in organisations.

The classification table in Block 1 in Table 28 shows that the hypothesised model has an overall predictive accuracy of 79.3%, a higher percentage than that of the basic model in Block 0, which displayed 72.1 %. The hypothesised model was exceptionally very accurate in predicting BDIDM adopters than non-adopters: 92.5% of adopters were accurately predicted compared to only 45.2% of non-adopters accurately predicted.

Table 25. Omnibus test (Whose significance indicate the significance of the regression)

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	31.149	8	.000
	Block	31.149	8	.000
	Model	31.149	8	.000

Table 26. Cox & Snell R Square test (Confidence interval)

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	100.335[a]	.245	.353

a. Estimation terminated at iteration number 5 because parameter estimates changed by less than .001.

Table 27. Significance Hosmer and Lemeshow test (Whose insignificance indicate the significance of the regression)

Hosmer and Lemeshow Test

Step	Chi-square	df	Sig.
1	8.476	8	.388

Table 28. Classification Table indicating TOE-BDIDM effectiveness: Predictive capabilities

Classification Table[a]

			Predicted		
			Adopt Indicator		Percentage
	Observed		Yes	No	Correct
Step 1	Adopt Indicator	Yes	74	6	92.5
		No	17	14	45.2
	Overall Percentage				79.3

a. The cut value is .500

Table 29. Wald statistics showing the significance of each element of the regression (test of the criticality of each factors)

Variables in the Equation

								95% C.I.for EXP(B)	
		B	S.E.	Wald	df	Sig.	Exp(B)	Lower	Upper
Step 1[a]	BDIDM_Char	-1.640	.705	5.415	1	.020	.194	.049	.772
	BDIDM_Read	-.167	.442	.142	1	.706	.847	.356	2.012
	Inf_Comp	-.318	.347	.837	1	.360	.728	.368	1.438
	Org_Char	-.312	.672	.215	1	.643	.732	.196	2.734
	Org_Read	1.316	.691	3.626	1	.057	3.730	.962	14.458
	Indu_Mark	-.280	.349	.643	1	.422	.756	.381	1.498
	Sup_Env	-.707	.725	.951	1	.329	.493	.119	2.041
	Reg_Env	-.494	.354	1.948	1	.163	.610	.305	1.221
	Constant	6.258	2.920	4.593	1	.032	522.069		.772

a. Variable(s) entered on step 1: BDIDM_Char, BDIDM_Read, Inf_Comp, Org_Char, Com_Proc, Org_Read, Indu_Mark, Sup_Env, Reg_Env.

Wald statistics in table 29 show the significance of each factor included in the regression, with the values of the 'B' column representing the values each factor can predict. A Yes value is predicted with positive values and a No value with negative values. The 'Exp(B)' displays precisely how much of the variance of each factor impact the outcome in the dependent variable, with a value greater than 1 indicating an increase of 1 unit and values less than 1 indicating decrease. It can be seen that only Org_Read factors can predict a 'Yes' in the Adopt Indicator, hence it has a positive impact on BDIDM adoption. This result means *the more* there is Organisation Financial Readiness and Organisation Awareness (Org_Read), *the more likely* an organisation will adopt BDIDM. The rest of the factors can predict a 'No' value in the Adopt Indicator, hence they have a negative impact on BDIDM adoption. In the Technology context, this means *the less* the level of (i) Security, Trialability, Complexity, Observability, Compatibility, and Integration (BDIDM_Char); (ii) Competences and inadequate IT infrastructure available (Comp_Infr); and (iii) technology readiness and standardisation (BDIDM_Read); *the more unlikely* an organisation will adopt BDIDM. In the organisational context, this means *the less* there is (i) Employees Linkage and Presence Product Champion, (ii) Top Management Support, Leadership, and Communication (Org_Char), *the more unlikely* an organisation will adopt BDIDM. In the context of the external environment, it means *the less* there is (i) Vendor Support, Skill Labour, and Consultants (Sup-Env); (ii) Government Regulation and Compliance with Standards (Reg-Env); (iii) Industry Pressure and Competition Intensity (Ind_Mark), *the more unlikely* an organisation will adopt BDIDM.

However, the column 'Sig' of Table 29 reveals that of all the above relationships, only BDIDM_Char's was statistically significant since it is the only factor displaying a p-value of less than .05 (Wald = 5.415, df = 1, Sig = .02). Therefore, BDIDM characteristics, which is made of Security, Trialability, Complexity, Observability, Compatibility, and Integration items, constitute the most significant factor that negatively impacts the likelihood of adopting BDIDM in an organisation. *The less* BDIDM is secure (Security), controllable (Observability), user-friendly (Trialability), easy to implement (Complexity), combinable with other systems (Compatibility), smoothly functioning in the organisational ecosystem (Integration); *the more unlikely* an organisation will adopt it.

As a result, of the eight underlying null hypotheses, only $H0_1$ was rejected, which confirmed the study's alternative hypothesis Ha_1 stating that BDIDM Characteristics have a statistically significant impact on BDIDM Adoption. As described in Table 36, the study failed to reject the null hypotheses $H0_{3,}$ $H0_4$, $H0_5$, $H0_6$, $H0_{8,}$ $H0_9$, and $H0_{10}$. This means there was not enough statistical evidence in the data to support Ha_3, Ha_4, Ha_5, Ha_6, Ha_8, Ha_9, and $Ha_{10.}$

4.1.3. Chi-Square tests of goodness of fit and association.

Chi-Square tests intended to test $H0_2$ and $H0_7$ as these were not part of the above logistic regression due to their nominal nature. This test was done in two steps: Chi-Square test of Goodness of fit (shown in Table 30 and 31) and Chi-Square test of association (shown in Table 32 and 33).

The first step in testing $H0_2$ and $H0_7$ was to assess the significance of the difference between categories for both Blockchain Type and Organisation Size variables, respectively represented $H0_{2.1}$ and $H0_{7.1}$. Table 30 show that the idea behind the null hypothesis $H0_{2.1}$ and $H0_{7.1}$ was that all categories are equal thus are expected to have equal frequencies: 37 for each of the three blockchain types and 27.8 for each of the four organisations sizes. Chi-Square test of Goodness of fit assessed the residuals between the expected and observed frequencies to see if they were due to a significant difference between the categories or simply a result of randomness. Table 31 reports a p-value of less than .05 for both Blockchain Type and Organisation Size variables, suggesting that the categories were indeed different.

Table 30. Chi-Square test of Goodness of fit - Count

Blockchain Type2

	Observed N	Expected N	Residual
Public permissionless blockchain	5	37.0	-32.0
Public permissioned blockchain	25	37.0	-12.0
Private permissioned blockchain	81	37.0	44.0
Total	**111**		

Organisation Size

	Observed N	Expected N	Residual
Micro Enterprise	6	27.8	-21.7
Small Enterprise	13	27.8	-14.7
Medium Enterprise	22	27.8	-5.7
Large Enterprise	70	27.8	42.3
Total	111		

Table 31. Chi-Square test of Goodness of fit - significance

Test Statistics

	Blockchain Type1	Organisation Size
Chi-Square	83.892[a]	90.405[b]
df	2	3
Asymp. Sig.	.000	.000

a. 0 cells (0.0%) have expected frequencies less than 5. The minimum expected cell frequency is 37.0.

b. 0 cells (0.0%) have expected frequencies less than 5. The minimum expected cell frequency is 27.8.

The next step in testing $H0_2$ and $H0_7$ was to assess the significance of the association between the categories and the outcome in the Adopt Indicator dependant variable, for both Blockchain Type and Organisation Type variables respectively represented by $H0_{2.2}$ and $H0_{7.2}$. The question was whether an organisation decided to adopt or not to adopt BDIDM based on its size or the blockchain type. Table 32 describes the count for adopters (‘Yes’) and non-adopters (‘No’) based on each organisation's size and blockchain type. Table 33 reports p-values of more than .5 for Organisation Size and less than .5 for Blockchain Type variables. These results suggest that only the Blockchain Type’s association with Adopt Indicator is statistically significant. There is not enough statistical evidence to support the existence of Organisation Size’s associations with Adopt Indicator. Therefore, an organisation can decide to adopt or not to adopt BDIDM based on the blockchain types.

Table 32. Chi-Square test of association - Count

Crosstabs

Count

		Organisation Size				Total
		Micro-Enterprise	Small Enterprise	Medium Enterprise	Large Enterprise	
Adopt Indicator	Yes	6	11	14	49	80
	No	0	2	8	21	31
	Total	6	13	22	70	111

		Blockchain Type2			Total
		Public permissionless blockchain	Public permissioned blockchain	Private permissioned blockchain	
Adopt Indicator	Yes	5	22	53	80
	No	0	3	28	31
	Total	5	25	81	111

Table 33. Chi-Square test of association - Significance

Chi-Square Tests

Organisation Size	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4.268[a]	3	.234
Likelihood Ratio	5.960	3	.114
Linear-by-Linear Association	2.295	1	.130
N of Valid Cases	111		

a. 3 cells (37.5%) have expected count less than 5. The minimum expected count is 1.68.

Blockchain Type2	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.863[a]	2	.032
Likelihood Ratio	8.692	2	.013
Linear-by-Linear Association	6.653	1	.010
N of Valid Cases	111		

a. 1 cells (16.7%) have expected count less than 5. The minimum expected count is 2.79.

Table 34. Summary hypothesis testing: two supported hypotheses (H0$_1$ and H0$_2$)

	Null hypothesis tested			Outcome
Technology	H0$_1$: BDIDM Characteristics do not have a statistically significant impact on BDIDM Adoption in organisations.			R
	H0$_2$:	H0$_{2.1}$: Statistically, Blockchain Types are equal.	R	R
		H0$_{2.2}$: Statistically, Blockchain Types are not associated with BDIDM adoption in organisations.	R	
	H0$_3$: BDIDM Readiness does not have a statistically significant impact on BDIDM Adoption in organisations.			FR
	H0$_4$: IT Infrastructure and Competencies do not have a statistically significant impact on BDIDM Adoption in organisations.			FR
Organisation	H0$_5$: Organisation Characteristics do not have a statistically significant impact on BDIDM Adoption.			FR
	H0$_6$: Organisation Readiness does not have a statistically significant impact on BDIDM Adoption.			FR
	H0$_{7:}$	H0$_{7.1}$: Statistically, Organisation Sizes are equal.	R	FR
		H0$_{7.2}$: Statistically, Organisation Sizes are not associated with BDIDM adoption in organisations.	FR	
Environment	H0$_8$: Industry and Market Environment do not have a statistically significant impact on BDIDM Adoption in organisations.			FR
	H0$_9$: Support Environment does not have a statistically significant impact on BDIDM Adoption in organisations.			FR
	H0$_{10}$: Regulatory Environment does not have a statistically significant impact on BDIDM Adoption in organisations.			FR
Note: R = Rejected, FR= Failed to Reject				

4.2. Discussion

This section briefly discusses the implication of the findings revealed in the analysis based on the research objectives and assumptions, attempting to understand the findings' practical significance from the literature review perspective.

4.2.1. Impact of the TOE factors on BDIDM adoption in organisations.

This study argued that TOE factors significantly impact the adoption of BDIDM in organisations positively or negatively. I was assumed there was a relationship between the TOE factors and BDIDM adoption in organisations. The findings revealed that the relationship exists, confirming that TOE factors impact how an organisation "identifies the need, searches, and adopts new technologies" (Baker, 2012, p. 232). It was also assumed that these factors would impact innovation adoption in organisations by either constraining or promoting it (Demir et al., 2020). They would predict BDIDM adopters and non-adopters. The result verified this assumption as one factor that had a positive impact, promoting BDIDM adoption, thus could predict BDIDM adopters. Seven had a negative impact, constraining BDIDM adoption, thus could predict BDIDM non-adopters.

The factor promoting the adoption was Organisation Readiness, made of Organisation Financial Readiness and Organisation Awareness items. Positive growth in the score of this group of items increases the likelihood of an organisation to adopt BDIDM. Hence, this factor could predict BDIDM adopters.

In the technological context, factors limiting the adoption were (i) BDIDM characteristics (Security, Trialability, Complexity, Observability, Compatibility, and integration), (ii) BDIDM Readiness (Technology Readiness and Standardisation of BDIDM), and (iii) Infrastructure and Competences (IT Infrastructure and BDIDM Competences). In the organisational context, the factor limiting the adoption was Organisation Characteristics (Employees Linkage, Presence of Product Champion, Top Management Support, and Leadership and Communication). Lastly, in the environmental context, factors limiting the adoption were (i) Industry and Market (Industry Pressure and Competition Intensity), (ii) Support Environment (Skills, Vendors and Consultants), and (iii) Regulatory Environment (Government Regulation and Compliance with Standards). Negative growth in the scores of these groups of items decreases the likelihood of an organisation to adopt BDIDM. Hence these factors could predict BDIDM non-adopters.

However, the data suggested that all the factors were statistically insignificant except for BDIDM Characteristics, representing Technology Characteristics in the TOE model. This finding verified the study's assumption indicating that some TOE factors were critical than others. Awa et al. (2016, p. 15) used the same methodology but in the context of the adoption of ERP solutions in SMEs. They found that Organisation Size ("Size of the firm") and Support Environment ("External support") were statistically significant at $p<.05$. This data did not support Ha7 and Ha$_9$, establishing that the impact of Organisation Size and Support Environment on BDIDM adoption in organisations were statistically insignificant. The data contrasted the literature suggestion of large enterprises being more likely to adopt BDIDM than SMEs (Clohessy & Acton, 2019) due to its relative cost of implementation (Demir et al., 2020). The insignificance of external support in the context of BDIDM might suggest that outsourcing IDM solutions is perhaps impractical for organisations than outsourcing ERP solutions in SMEs. This is possibly due to privacy issues and the legal responsibilities involved in IDM (Bernabe et al., 2019; Mpofu & van Staden, 2017).

4.2.2. Most critical factors of the TOE model in the context of BDIDM

This study argued that some TOE factors were more critical than others, assuming they were statistically significant and impacted BDIDM adoption the most. The data suggested that this argument, alongside the assumption, is correct as two factors were identified as the most critical BDIDM adoption in organisations, one of which was statistically significant.

The first most critical factor was BDIDM Characteristics since it was the only statistically significant factor in the regression model. The data provided enough evidence supporting that the more BDIDM is insecure, uncontrollable, user-unfriendly, complex, incompatible with other systems, and challenging to integrate the enterprise ecosystem, the less likely an organisation would adopt it.

The significance of BDIDM Characteristics resonates with the literature portraying BDIDM as a disruptive technology and 'radical' innovation. As Baker mentioned when describing radical innovation, BDIDM tends to render existing IDM and related competencies obsolete. Baker added that instead of an incremental or synthetic change, radical innovation tends to produce discontinuous change. Indeed, BDIDM does not create new versions of existing technologies but tends to replace existing centralised IDM systems by combining other technologies in a radical manner of distributed computing (Grüner et al., 2019). Blockchain tends to shift the security paradigm by assuming "the presence of adversaries in the network" (Shetty et al., 2019, p. XIII). BDIDM might have both a high risk related to its adoption and the potential to "enhance competitive standing in an organisation" (Baker, 2012, p. 232). Hence the criticality of BDIDM Characteristics for its adoption and broadly the Technology Characteristics aspects of adopting disruptive technologies.

The literature review showed that critics of BDIDM like SSI supported its impracticality in organisations by highlighting its principle vulnerability dwelling at its endpoints (Helebrandt et al., 2018). Some even questioned whether further adoption of blockchain-based solutions should be encouraged and whether the overall potential for change "could be net positive" (Rot & Blaicke, 2019, p. 447). The significance of BDIDM Characteristics may logically imply more investment toward getting BDIDM more secure, controllable, user-friendly, less complex to implement, compatible with other systems and smooth to integrate the enterprise ecosystem. However, some of these goals might be extremely difficult, if not nearly impossible, to achieve since blockchain was somehow designed to function as such. Blockchain implementation cost is high, requiring radically different infrastructure and a highly skilled team (Demir et al., 2020). But given the BDIDM's cost savings in password management alone estimated by Wolfond (2017) in the millions and the rise of the Zero Trust architecture endorsing radical IDM (Stafford, 2020), the question might be perhaps shifting from 'how to get BDIDM organisation friendly to 'how to get an organisation BDIDM friendly'. Demir et al. corroborate by stating that "reluctance to adopt disruptive technologies might be a significant competitive disadvantage for an organisation, whereas proactive planning can be a significant advantage" (p. 34).

From a practical significance perspective, the second most critical factor was Organisation Readiness, made of Financial Readiness and Organization Awareness items. Although Organisation Readiness was not statistically significant, it was remarkably the least statistically insignificant of all, with a p-value of .57, just above the threshold of .5. Since this factor was the only one that had a positive impact on BDIDM adoption, its second importance echoes the so highlighted financial resources criticality in adopting Blockchain-based solutions (Demir et al., 2020). Moreover, the relative newness of BDIDM impact on its adoption was reoccurring in the literature review, suggesting the importance of organization awareness about BDIDM in promoting its adoption (Upadhyay, 2020).

4.2.3. Association of Blockchain Types with BDIDM adoption in organisations

Another result that verified the assumption about the significance of some TOE factors over others was the individual statistically significant impact of the Blockchain Type item on BDIDM adoption. The Chi-Square tests confirmed a statistically significant difference between blockchain types (i.e., public permissionless, public permissioned, and private permissioned blockchains) and their association with BDIDM adoption in organisations. The data provided solid evidence supporting that an organisation can adopt BDIDM because of the type of blockchain involved. It is important to note that the Blockchain Type item was designed as part of the BDIDM Characteristic factor, which was already statistically significant in the regression model. This shows a good extend of consistency in the measurements and validity of the results.

The significance of the Blockchain Type item echoes the intense debate in the literature around the practicality of BDIDM for the enterprise context. The debate involved questions around which type of blockchain should be suitable for an organisation as opposed to individual use on the internet (Wüst & Gervais, 2018). Some researchers suggested public permissioned blockchains perceiving them as more balanced versions of blockchains (Buccafurri et al., 2018). Indeed, these blockchains are claimed to be more decentralized, scalable, efficient (Thai et al., 2019) and offer “privacy protection and high transparency”(Mitani & Otsuka, 2020, p. 21573). Others complemented that public permissioned blockchains were seemingly ideal for BDIDM-SSI (Bernabe et al., 2019). Still, others argued that private permissioned blockchain might be the perfect implementation for ‘enterprise BDIDM’ because it endorses a service-centric approach by giving total control of the system to the identity provider called “Trust Anchor”(Marsalek et al., 2019, p. 46).

This debate was also apparent in the data. Descriptive statistics showed that 72.1% of respondents intended to adopt BDIDM while 27.9% did not. Yet, 66.7% of respondents preferred private permissioned blockchain, 24.3 % public permissioned blockchain, and 9% public permissionless blockchain. Thus, adopters might be referring to a particular type of blockchain than the other, in this case, private permissioned blockchain since it was the most preferred. Considering Bernabe et al. (2019)’s suggestion of BDIDM-SSI fitting into public permissioned blockchain, the data is perhaps suggesting that BDIDM-SSI is not fully practical for the enterprise context. The majority of respondents preferred private permissioned blockchain, which tends to be less decentralised, disintermediated, and privacy-preserving, supporting Marsalek et al. (2019)’s perspective over Buccafurri et al. (2018), Thai et al. (2019), and Mitani and Otsuka (2020)’s.

4.1.1. Effectiveness and Appropriateness of the TOE-BDIDM

Part of the study’s argument was that the TOE model was effective and appropriate for investigating the phenomenon. The binary logistic regression modelling revealed that TOE-BDIDM was excellent in predicting BDIDM adopters at an accuracy rate of 92.5%. The model was found arguably fair in predicting non-adopters of BDIDM at an accuracy rate of 45.2%. The TOE-BDIDM’s overall predictive accuracy set at 79.3%. These results are valid since Awa et al. (2016)’s TEO-based model displayed a similar pattern, with about same overall predictive accuracy of 78.7% but at different individual proportions of 87.1% for ERP Adopters and 66.7% for ERP Non-adopters.

Concerning TOE-BDIDM’s appropriateness, the SEM of the measurement model performed on data suggested a poor fit. After some modification by eliminating poor loading factors, adding few covariances among some error terms, and solving ‘redundancy’, the modified model better fitted the data. The presumed redundancy issue also affected the model's convergent validity. However, the issue seemed to result from a misalignment of a particular variable than multiclonality. The coloniality test identified no redundant variable or redundant constructs, indicating acceptable discriminant validity. Most of the items were loading well on the constructs, suggesting fair composite reliability. Nearly the entire model had an excellent internal consistency, even for the constructs made of two items. Therefore, it was concluded that TOE-BDIDM was relatively appropriate for the BDIDM context.

Another observation about the appropriateness of TOE to the context of BDIDM was its explanatory capabilities. The TOE-BDIDM identified two significant relationships with N=111, at p<.05 compared to three identified by Awa et al. (2016) with N=373, at p<.05. This observation verified the study's assumption that BDIDM adoption in organisations could be explained using the TOE theory. The observation also confirmed the validity of the TOE's interoperability claimed by Baker (2012) when claiming that the theory has "broad applicability and possesses explanatory power" (p. 151) across various technological, industrial, and national/cultural contexts.

Moreover, the findings of the significance of BDIDM Characteristics factor and Blockchain Type item tend to suggest that the adoption of BDIDM might be "more driven by technological factors than by organizational and environmental factors" (Awa et al., 2016, p. 16), just like was Awa et al. (2016)'s about the adoption of ERP by SMEs. Hence it was reasonable to consider the entire TOE model instead of the organisation context only. Indeed, some studies found the Organisational context to be "the most significant determinant of IT innovation adoption in organisations" (Clohessy & Acton, 2019, p. 1457). But Srivastava et al. (2020) recommended introducing technological perspectives in the study of innovation adoption in organisations as this context was often neglected in the past. Hence, the choice of TOE over TAM, TPB, UTAUT and TRI was reasonable.

However, the TOE's flexibility allowing for customisation to different contexts (Baker, 2012) tended to leave room for ambiguities. The unexpected discovery about the misalignment of the Support Environment factor could help illustrate the supposed ambiguity. The literature suggested diverging views about the Skills, Vendors, and Consultants items that made up the Support Environment factor in this study. Awa et al. (2016) referred to them as "Technical Know-how" (p. 7) thus located them under the Technology contract. Baker (2012) identified them as external support thus located them under the Environment construct. This study initially opted for the latter suggestion, which was proved unfit for this data. Contrary to both views, the data suggested that the group of items fit the Organisation construct well. Hence the modified model for further research to attest.

An additional 'negative' observation about TOE appropriateness to BDIDM adoption in organisations was its lack of a 'User context'. BDIDM, like SSI, tend to involve a great deal of trust in users. In contrast to traditional IDM systems that are often organisation-centric, SSI is user-centric (Grüner et al., 2019). Due to the privacy requirement involved in SSI, users would be self-managing their IDs (Bernabe et al., 2019; Kshetri, 2017). Self-IDM might be risky for organisations as it "could practically introduce novel issues" (Maesa & Mori, 2020, p. 106) and bring a heavy responsibility on users to "safeguard against forgetting (or losing) the private key" (Kuperberg, 2019, p. 5). A complete explanation of BDIDM adoption in organisations might necessitate measuring the individual factors in addition to the technological, organisational, and environmental factors. Individual factors for BDIDM adoption could include user preparedness, willingness, acceptance, skill, awareness, perceived usefulness, etc. Therefore, TOE might not fully represent the organisational context of innovation adoption as suggested by Baker (2012), especially regarding adoption of disruptive innovation like BDIDM-SSI.

4.2. Chapter summary

The first section of this chapter reported the statistical analysis of the primary data collected using the TOE-BDIDM to help reach the study's objectives. The section provided results of data cleaning done to enforce the sample frame, ethical requirement, and deal with outliers; then gave the background information about the sample. It then tested the model fitness, reliability, and validity through Cronbach's Alpha and CFA. It followed with testing of the distributions' normality. It then moved to hypothesis testing using logistic regression modelling and Chi-square tests, summarizing the outcome in Table 34.

The second section of this chapter discussed the implications of the findings, considering the research questions, objectives, assumptions and attempting to understand the finding's practical significance from the literature review perspectives. It highlighted various implications, some relating to the disruptiveness nature of BDIDM and others pertaining to the

BDIDM adoption being more driven by technological than organisational or environmental contexts

CHAPTER 5: CONCLUSION

This study primarily sought to explain how TOE factors affected the decision to adopt BDIDM in organisations to determine which factor was the most critical. This was about first determining whether relationships existed between the factors and the dependent variable, second the nature and significance of each factor in the model, and third which the most critical factor was. In addition, the study sought to determine if blockchain implementation types had any significant individual impact on BDIDM adoption in organisations. Moreover, the study aimed to determine the appropriateness and effectiveness of TOE-BDIDM to see if it accurately predicted BDIDM adopters and non-adopters, fitted the data well, and was suitable for investigating the phenomenon. The following sections summarise the study's findings, provide limitations and recommendations for further research.

5.1. Summary of findings

The binary logistics regression modelling performed on data confirmed a relationship between the TOE factors and BDIDM adoption. They predicted whether an organisation would fall under the BDIDM adopters or non-adopters category. The impact of each of the TOE factors on BDIDM adoption was either positively or negatively. A positive predictor suggested that positive growth in the factor's score results in an increased likelihood of an organization to adopt BDIDM. A negative predictor suggested that negative growth in the factor's score results in a decreased chance of an organisation to adopt BDIDM. However, BDIDM Characteristics was the only statistically significant factor in the regression model. The data provided solid evidence supporting that the more BDIDM is insecure, uncontrollable, user-unfriendly, complex, incompatible with other systems, and challenging to integrate the enterprise ecosystem, the less likely an organisation would adopt it. Therefore, Technology Characteristics was the first most critical factor, the most that could predict BDIDM non-adopters. Organisation Readiness was arguably the second most critical since it was the less insignificant in the regression model and the most that could predict BDIDM adopters

Another statistically significant result was found between blockchain types and BDIDM adoption. The Chi-Square tests confirmed a statistically significant difference between blockchain types (i.e., public permissionless, public permissioned, and private permissioned blockchains) and their statistical significant association with BDIDM adoption in organisations. The data provided solid evidence supporting that an organisation can adopt BDIDM because of the type of blockchain involved.

TOE-BDIDM was very effective in predicting adopters than non-adopters of BDIDM, accurately predicting 92.5% of adopters and 45.2% of non-adopters. Confirmatory factor analysis suggested that TOE-BDIDM tended to be faulty on construct validity since it did not perfectly fit the data, possibly due to some poorly loading items and misalignment of a construct. However, the model had excellent internal reliability, good construct reliability, and arguably reasonable convergent and Discriminant validity. Hence, the general view was that the model was relatively appropriate for investigating the phenomenon.

The above view was also motivated by the model's explanatory capabilities even in the BDIDM context. It identified a reasonable number of significant relationships compared to a similar study done by Awa et al. (2016) that relatively larger sample size. However, the TOE's flexibility feature appeared to accommodate some ambiguities. The TOE theory was also found arguably 'incomplete' as it does not include any individual aspects of the adoption, which seems critical for adopting BDIDM like SSI in organisations.

5.2. Limitations

A reflection on the research process recognised limitations linked to methodology, theory, researchers' experience, and literature review.

At the methodological level, the first limitation was the philosophical choice of positivism and quantitative methods, which did not allow for deeper insights into the current state of BDIDM adoption in South African organizations. Although this was due to the relative newness of the technology involved, which made the study prioritise prediction over history, a different approach would yield different results. The second limitation was about methods of data analysis. It was impossible to test the structure model of TOE-BDIDM using path analysis as suggested by the SEM framework. This was due to the dependent variable's nature, which was binary instead of continuous or interval, intentionally set according to the study objective. The third limitation was the relatively small sample size which was unexpected and appeared to be linked to the unique circumstances of COVID-19 in which data was collected. Since some model fitness tests heavily rely on the sample size, a bigger sample would yield an even better TOE-BDIDM fit to the data.

At the theoretical level, the key limitation was that the theoretical framework used, based on the TOE theory, was found to some extent incomplete. Although it was more suitable for the context than other theories found in the literature, it did not accommodate measures of the individual aspects of BDIDM adoption in organisations, which might be key for a smooth adoption of this disruptive technology.

At the researchers' experience level, there were some inconsistencies due to human error. The most noticeable limitation in this category was that User Privacy was missing from the interval scaled data because it was unintentionally omitted in data collection. Hence, Privacy was only measured on a binary scale, making it impossible to be part of regression analysis and SEM of the measurement model.

At the literature review level, the principal limitation was that not all potential papers were included in the sample. Firstly, because of the diversity in blockchain applications and the high interest resulting in hundreds of articles published mainly in the last free years from the time of writing. The review needed to stay as focused on the topic as possible. Second, because the topic involves various concepts from both IDM and blockchain: the study tried to limit the sample strictly to the scope of the review. Hence, some papers were excluded though they were satisfactory to some selection criteria. However, researchers were confident they saturated the topic because there was a repetition of what had already been lent.

5.3. Further research

Given the limitations highlighted above, methodological, theoretical, and topical measures could be adopted for further research on the topic or in the field.

From a methodological perspective, as blockchain technology evolves, further research might consider using a different approach in the research design, including combining quantitative and qualitative data collection and analysis methods, to accommodate both depths and accuracy. Alternatively, one might want to record the actual state of BDIDM adoption in a specific context, for instance, using a case study research strategy rather than a survey.

From a theoretical perspective, future investigation of adoption of disruptive technologies like BDIDM SSI might consider combining the TOE with another theoretical framework, such as TAM, to include the individual aspects of adoption in organisations. Alternatively, one might use any other theory, if necessary develop one, that provides for all the four contexts: Technology, Organisation, External Environment, and ‘User’.

From a topical perspective, the reflection done on this work led to an understanding that a sustainable BDIDM adoption might be beyond organisations. It was leant that, given its relatively high disruption, some forms of BDIDM might perhaps be impractical for sole organisations to adopt without a national strategy supporting and/or enforcing the adoption. The government might need to be actively involved, if not the initiator of the adoption. This might be the case with national identity management, for which silos of BDIDM adoption might be ineffective, if not illegal in some instances. Therefore, future research might instead study the nationwide adoption of BDIDM, more broadly the institutionalisation of blockchain.

REFERENCES

Agresti, A., & Finlay, B. (2009). *Statistical methods for the social sciences* (Fith Edition ed.). Pearson Education Limited.

Ahmad, S., Zulkurnain, N. N. A., & Khairushalimi, F. I. (2016). Assessing the validity and reliability of a measurement model in Structural Equation Modeling (SEM). *Journal of Advances in Mathematics and Computer Science*, 1-8.

Ahmed, M., Elahi, I., Abrar, M., Aslam, U., Khalid, I., & Habib, M. A. (2019). Understanding blockchain: Platforms, applications and implementation challenges. Proceedings of the 3rd International Conference on Future Networks and Distributed Systems,

Alexander, D., Finch, A., Sutton, D., & Taylor, A. (2020). *Information security management principles* (Third Edition ed.).

Awa, H. O., Ukoha, O., & Emecheta, B. C. (2016). Using TOE theoretical framework to study the adoption of ERP solution. *Cogent Business & Management*, *3*(1), 1196571.

Awang, Z. (2015). *SEM made simple: A gentle approach to learning Structural Equation Modeling*. MPWS Rich Publication.

Baars, D. (2016). *Towards self-sovereign identity using blockchain technology* University of Twente].

Baker, J. (2012). The Technology–Organization–Environment framework. In *Information systems theory*. (Vol. 28, pp. 231). Springer. https://doi.org/doi:10.1007/978-1-4419-6108-2_12

Bendiab, K., Kolokotronis, N., Shiaeles, S., & Boucherkha, S. (2018). WiP: A novel blockchain-based trust model for cloud identity management. 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech),

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological bulletin*, *107*(2), 238.

Bentler, P. M., & Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological bulletin*, *88*(3), 588.

Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access*, *7*, 164908-164940.

Blunch, N. (2012). *Introduction to structural equation modeling using IBM SPSS statistics and AMOS*. Sage.

Bollen, K. A. (1989). A new incremental fit index for general structural equation models. *Sociological Methods & Research*, *17*(3), 303-316.

Bouras, M. A., Lu, Q., Zhang, F., Wan, Y., Zhang, T., & Ning, H. (2020). Distributed ledger technology for eHealth identity privacy: State of the art and future perspective. *Sensors*, *20*(2), 483.

Breuer, J., Ranaivoson, H., Buchinger, U., & Ballon, P. (2015). Who manages the manager? Identity management and user ownership in the age of data. 2015 13th Annual Conference on Privacy, Security and Trust (PST),

Brown, M. W., & Cudeck, R. (1993). Alternative ways of assessing model fit. *Testing structural equation models*, *154*, 136-162.

Brown, T. A. (2015). *Confirmatory factor analysis for applied research*. Guilford publications.

Buccafurri, F., Lax, G., Russo, A., & Zunino, G. (2018). Integrating digital identity and blockchain. OTM Confederated International Conferences" On the Move to Meaningful Internet Systems", Butijn, B.-J., Tamburri, D. A., & Heuvel, W.-J. v. d. (2020). Blockchains: a systematic multivocal literature review. *ACM Computing Surveys (CSUR)*, *53*(3), 1-37.

Chakravarty, D., & Deshpande, T. (2018). Blockchain-enhanced Identities for Secure Interaction. 2018 IEEE International Symposium on Technologies for Homeland Security (HST),

Charanya, R., & Aramudhan, M. (2016). Survey on access control issues in cloud computing. 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS),

Clara, S., Huang, C., Gong, X., & Shenzhen (2014). *Distributed storage method, apparatus, and system for reducing a data loss that may result from a single-point failure* U. s. patent.

Clohessy, T., & Acton, T. (2019). Investigating the influence of organizational factors on blockchain adoption: An innovation theory perspective. *Industrial Management & Data Systems*.

Cramer, D. (2003). *Fundamental statistics for social research: step-by-step calculations and computer techniques using SPSS for Windows*. Routledge.

Cui, Z., Fei, X., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A hybrid BlockChain-based identity authentication scheme for multi-WSN. *IEEE Transactions on Services Computing*, *13*(2), 241-251.

Daoud, J. I. (2017). Multicollinearity and regression analysis. Journal of Physics: Conference Series,

DeCoster, J. (1998). Overview of factor analysis. In: Tuscaloosa, AL.

Demir, M., Turetken, O., & Mashatan, A. (2020). An Enterprise Transformation Guide for the Inevitable Blockchain Disruption. *Computer*, *53*(6), 34-43.

Doane, D. P., & Seward, L. E. (2011). Measuring skewness: a forgotten statistic? *Journal of statistics education*, *19*(2).

Dresher, D. (2017). Blockchain Basics. *Apress, Frankfurt*.

Duy, P. T., Hien, D. T. T., Hien, D. H., & Pham, V.-H. (2018). A survey on opportunities and challenges of Blockchain technology adoption for revolutionary innovation. Proceedings of the Ninth International Symposium on Information and Communication Technology,

El Madhoun, N., Hatin, J., & Bertin, E. (2019). Going beyond the blockchain hype: In which cases are blockchains useful for it applications? 2019 3rd Cyber Security in Networking Conference (CSNet),

Feng, B., Huang, C., & Gong, X. (2014). Distributed storage method, apparatus, and system for reducing a data loss that may result from a single-point failure. In: Google Patents.

Fernando, E. (2019). Essential Blockchain Technology Adoption factors in Pharmaceutical Industry. 2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE),

Finfgeld-Connett, D. (2018). *A guide to qualitative meta-synthesis*. Routledge.

Grassi, P., Fenton, J., Lefkovitz, N., Danker, J., Choong, Y.-Y., Greene, K., & Theofanos, M. (2017). *Digital identity guidelines: Enrollment and identity proofing*.

Grüner, A., Mühle, A., & Meinel, C. (2019). An Integration Architecture to Enable Service Providers for Self-sovereign Identity. 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA),

Hair, E., Halle, T., Terry-Humen, E., Lavelle, B., & Calkins, J. (2006). Children's school readiness in the ECLS-K: Predictions to academic, health, and social outcomes in first grade. *Early Childhood Research Quarterly*, *21*(4), 431-454.

Hameed, M. A., & Arachchilage, N. A. G. (2020). A Conceptual Model for the Organizational Adoption of Information System Security Innovations. In *Security, Privacy, and Forensics Issues in Big Data* (pp. 317-339). IGI Global.

Helebrandt, P., Bellus, M., Ries, M., Kotuliak, I., & Khilenko, V. (2018). Blockchain adoption for monitoring and management of enterprise networks. 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON),

Hinton, P., McMurray, I., & Brownlow, C. (2014). *SPSS explained*. Routledge.

Hufstetler, W. A., Ramos, M. J. H., & Wang, S. (2017). Nfc unlock: Secure two-factor computer authentication using nfc. 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS),

IBM-Security. (2019). IBM: Cost of a data breach report 2019. *Computer Fraud & Security*. https://doi.org/doi:10.1016/s1361-3723(19)30081-8

Ismael, S. N. a., Mohd, O., & Abd Rahim, Y. (2021). Assessing Data Sharing's Model Fitness Towards Open Data by using Pooled CFA. *International Journal of Advanced Computer Science and Applications (IJACSA), 12, No. 5*.

ISO/IEC. (2014). South african national standard: Information technology — security techniques — code of practice for information security controls. In. Switzerland: SABS.

Jöreskog, K., & Sörbom, D. (1984). LISREL-VI user's guide 3rd edn. *IN: Scientific Software, Mooresville*.

Kamble, S., Gunasekaran, A., & Arha, H. (2019). Understanding the Blockchain technology adoption in supply chains-Indian context. *International Journal of Production Research*, *57*(7), 2009-2033.

Karamchandani, A., Srivastava, S. K., & Srivastava, R. K. (2020). Perception-based model for analyzing the impact of enterprise blockchain adoption on SCM in the Indian service industry. *International Journal of Information Management*, *52*, 102019.

Karanja, E., & Rosso, M. A. (2017). The chief information security officer: An exploratory study. *Journal of International Technology and Information Management*, *26*(2), 23-47.

Kim, H., Kim, S.-H., Hwang, J. Y., & Seo, C. (2019). Efficient privacy-preserving machine learning for blockchain network. *IEEE Access*, *7*, 136481-136495.

Kim, T. K., & Park, J. H. (2019). More about the basic assumptions of t-test: normality and sample size. *Korean journal of anesthesiology*, *72*(4), 331.

Kiran, M. A., Yogeshwari, P., Bhavani, K. V., & Ramya, T. (2018). Biometric authentication: A holistic review. 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference on,

Kolb, J., AbdelBaky, M., Katz, R. H., & Culler, D. E. (2020). Core concepts, challenges, and future directions in blockchain: a centralized tutorial. *ACM Computing Surveys (CSUR)*, *53*(1), 1-39.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications policy*, *41*(10), 1027-1038.

Kuperberg, M. (2019). Blockchain-based identity management: A survey from the enterprise and ecosystem perspective. *IEEE Transactions on Engineering Management*, *67*(4), 1008-1027.

Kyriazos, T. A. (2018). Applied psychometrics: sample size and sample power considerations in factor analysis (EFA, CFA) and SEM in general. *Psychology*, *9*(08), 2207.

Labazova, O. (2019). Towards a Framework for Evaluation of Blockchain Implementations. ICIS, Liu, Y., Sun, G., & Schuckers, S. (2019). Enabling Secure and Privacy Preserving Identity Management via Smart Contract. 2019 IEEE Conference on Communications and Network Security (CNS),

Lopez, P. G., Montresor, A., & Datta, A. (2019). Please, do not decentralize the Internet with (permissionless) blockchains! 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS),

Ma, X. (2015). Managing identities in cloud computing environments. 2015 2nd International Conference on Information Science and Control Engineering,

Maesa, D. D. F., & Mori, P. (2020). Blockchain 3.0 applications survey. *Journal of Parallel and Distributed Computing*, *138*, 99-114.

Marky, K., Mayer, P., Gerber, N., & Zimmermann, V. (2018). Assistance in Daily Password Generation Tasks. Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers,

Marsalek, A., Kollmann, C., Zefferer, T., & Teufl, P. (2019). Unleashing the full potential of blockchain technology for security-sensitive business applications. 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC),

Marsh, H. W., & Hocevar, D. (1985). Application of confirmatory factor analysis to the study of self-concept: First-and higher order factor models and their invariance across groups. *Psychological bulletin*, *97*(3), 562.

Michael, S., & Anna, Z. J. (2019). An identity provider as a service platform for the edugain research and education community. 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM),

Mitani, T., & Otsuka, A. (2020). Traceability in permissioned blockchain. *IEEE Access*, *8*, 21573-21588.

Moghaddam, F. F., Wieder, P., & Yahyapour, R. (2017). A policy-based identity management schema for managing accesses in clouds. 2017 8th International Conference on the Network of the Future (NOF),

Mpofu, N., & van Staden, W. J. (2017). Evaluating the severity of trust to identity-management-as-a-service. 2017 Information Security for South Africa (ISSA),

Musuva-Kigen, P., Mueni, F., & Ndegwa, D. (2016). Africa cyber security report 2016. *Serianu Cyber Threat Intelligence Team*.

Mwenya, J. K., & Brown, I. Cloud privacy and security issues beyond technology: championing the cause of accountability.

Ngwenyama, O. (2019). The Ten Basic Claims of Information Systems Research: An Approach to Interrogating Validity Claims in Scientific Argumentation. *Available at SSRN 3446798*.

Oosterwyk, G., Brown, I., & Geeling, S. (2019). A Synthesis of Literature Review Guidelines from Information Systems Journals. Proceedings of 4th International Conference on the,

Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing*.

Post, R., Smit, K., & Zoet, M. (2018). Identifying factors affecting blockchain technology diffusion.

Pranata, S., & Nugroho, H. T. (2019). 2FYSH: two-factor authentication you should have for password replacement. *Telkomnika*, *17*(2), 693-702.

Queiroz, M. M., & Wamba, S. F. (2019). Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. *International Journal of Information Management*, *46*, 70-82.

Rauscher, T. G. (2005). Raid system with multiple controllers and proof against any single point of failure. In: Google Patents.

Romney, M., Steinbart, P., Mula, J., McNamara, R., & Tonkin, T. (2012). *Accounting Information Systems Australasian Edition*. Pearson Higher Education AU.

Rot, A., & Blaicke, B. (2019). Blockchain's future role in cybersecurity. analysis of defensive and offensive potential leveraging blockchain-based platforms. 2019 9th International Conference on Advanced Computer Information Technologies (ACIT),

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (5th ed.). Pearson (Intl).

Saunders, M. N., Lewis, P., Thornhill, A., & Bristow, A. (2016). *Research methods for business students* (7th ed.). Pearson (Intl).

Saunders, M. N., Lewis, P., Thornhill, A., & Bristow, A. (2019). *Research Methods for Business Students*. (8th ed.). Pearson (Intl)

Seitz, T., Mathis, F., & Hussmann, H. (2017). The bird is the word: a usability evaluation of emojis inside text passwords. Proceedings of the 29th Australian Conference on Computer-Human Interaction,

Shehu, A.-S., Pinto, A., & Correia, M. E. (2019). Privacy Preservation and Mandate Representation in Identity Management Systems. 2019 14th Iberian Conference on Information Systems and Technologies (CISTI),

Shetty, S., Kamhoua, C. A., & Njilla, L. L. (2019). *Blockchain for distributed systems security*. John Wiley & Sons.

Sohrabi, N., Yi, X., Tari, Z., & Khalil, I. (2020). BACC: blockchain-based access control for cloud data. Proceedings of the Australasian Computer Science Week Multiconference,

Stafford, V. (2020). Zero Trust Architecture. *NIST Special Publication*, *800*, 207.

stats-sa. (inedi). *Industry code list*. Retrieved 24 September 2020 from http://www.statssa.gov.za/?page_id=4519

Tanaka, J. S., & Huba, G. J. (1985). A fit index for covariance structure models under arbitrary GLS estimation. *British journal of mathematical and statistical psychology*, *38*(2), 197-201.

Thai, Q. T., Yim, J.-C., & Kim, S.-M. (2019). A scalable semi-permissionless blockchain framework. 2019 International Conference on Information and Communication Technology Convergence (ICTC),

Thakkar, J. J. (2020). *Structural Equation Modelling: Application for Research and Practice (with AMOS and R)*. Springer Singapore Pte. Limited.

Thota, A. R., Upadhyay, P., Kulkarni, S., Selvam, P., & Viswanathan, B. (2020). Software Wallet Based Secure Participation in Hyperledger Fabric Networks. 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS),

Thrane, C. (2019). *Applied Regression Analysis: Doing, Interpreting and Reporting*. Routledge.

Trafimow, D., Wang, T., & Wang, C. (2019). From a sampling precision perspective, skewness is a friend and not an enemy! *Educational and Psychological Measurement*, *79*(1), 129-150.

Upadhyay, N. (2020). Demystifying blockchain: A critical analysis of challenges, applications and opportunities. *International Journal of Information Management*, *54*, 102120.

Vogt, W. P., & Johnson, R. B. (2015). *The SAGE dictionary of statistics & methodology: A nontechnical guide for the social sciences*. Sage publications.

Walsh, D., & Downe, S. (2005). Meta-synthesis method for qualitative research: a literature review. *Journal of Advanced Nursing*, *50*(2), 204-211. https://doi.org/10.1111/j.1365-2648.2005.03380.x

Wheaton, B. (1987). Assessment of fit in overidentified models with latent variables. *Sociological Methods & Research*, *16*(1), 118-154.

Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security sixth edition*. Cengage Learning.

Wolfond, G. (2017). A blockchain ecosystem for digital identity: improving service delivery in Canada's public and private sectors. *Technology Innovation Management Review*, *7*(10).

Wooditch, A., Johnson, N. J., Solymosi, R., Ariza, J. M., & Langton, S. (2021). The Normal Distribution and Single-Sample Significance Tests. *A Beginner's Guide to Statistics for Criminology and Criminal Justice Using R*, 155-168.

Wüst, K., & Gervais, A. (2018). Do you need a blockchain? 2018 Crypto Valley Conference on Blockchain Technology (CVCBT),

Xiaofeng, L., Shengfei, Z., & Shengwei, Y. (2019). Continuous authentication by free-text keystroke based on CNN plus RNN. *Procedia computer science*, *147*, 314-318.

Zhu, X., & Badr, Y. (2018). A survey on blockchain-based identity management systems for the Internet of Things. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),

APPENDIX

Appendix 1: Consent form

Request for research participation

Dear prospective participant,

In terms of the requirements for completing a master’s degree in Information Systems at the University of Cape Town, a research study is required. The researcher, Sarah Mulombo Mulaji, has chosen to conduct a study entitled "Adoption of Blockchain-based Distributed Identity Management (BDIDM) in Organisations".

This research has been approved by the Ethics in Research Committee of the faculty of Commerce.

Identity management, which consists of identification and authentication of users of a digital system (for instance, a corporate website, a database, an app, etc.), is a vital information security (InfoSec) control that restricts access to the system to legitimate users only. Identity management contributes to preventing security breaches. Unfortunately, ongoing data breaches in organisations indicate that current identity management systems face challenges that need to be addressed. This research investigates the adoption of Blockchain to mitigate some of those challenges in organisations potentially. The primary aim is to verify whether the technological, organisational, and external environmental factors impact the adoption and determine the most critical factors.

If you are working within South Africa and your work involves some aspects of information & cybersecurity of your organisation, this survey is targeted to you. The online questionnaire is designed in such a way to ensure the anonymity of your response. You will not be requested to supply any personal identifiable information. Your participation in this research is voluntary.

If you are willing to participate in this study, please click on the ‘Next’ button to proceed with the questionnaire. The questionnaire is made of 14 multiple-choice questions and will take approximately 15 minutes to complete. You can choose to withdraw from the questionnaire at any stage for whatever reason, in accordance with ethical research requirements.

Should you have any questions regarding this research, please feel free to contact the researcher via email: mljsar001@myuct.ac.za

Your participation in this study would be greatly appreciated.

Sincerely,

Researcher: Sarah Mulombo Mulaji
Supervisor: Dr Sumarie Roodt

Appendix 2: Data collection instrument

ITEM	SURVEY QUESTION
SECTION A: DEMOGRAPHIC INFORMATION	
Country	Country
Age	Please select your age group
Job title	Please select your job title
Organisation sector	Please select your organisation sector
Number of employees	Please select your organisation size (number of employees)
Existence of IDM	Does your organisation have an established identity (and access) management system?
Type of existing IDM	Which, among the following, is the type(s) of your organisation's identity (and access) management system currently used? PLEASE SELECT ALL APPLICABLE ○ Centralised: Needs a central component to function, e.g., Radius, Kerberos, etc. ○ ID-as-a-Service: centralised in the cloud, e.g., Okta, AWS-IAM, etc. ○ Federated: Cross-domain/single-sign-on, e.g., OpenID, SAM, Auth, etc. ○ Distributed: No need for central component, e.g., no sever to store user credentials
Awareness1	Is your organisation, or are you, aware of blockchain-based identity management?
SECTION B: TECHNOLOGY CONTEXT	
Barriers *Benefits*	Which among the following do you consider as either a benefit (STRENGTH) or a drawback (WEAKNESS) of/about Blockchain-based distributed Identity Management in organisations? A 'strength' would promote the adoption of BDIDM while a 'weakness' would prevent the adoption of BDIDM
Blockchain Type	Which of the following type of blockchains do you think is the most suitable for an enterprise context? ○ PUBLIC PERMISSIONLESS: Not restricted. Anyone can join the blockchain, and users self-manage their data and have full control over it. ○ PUBLIC PERMISSIONED: Somewhat restricted. Some users can join the blockchain. Users self-manage their data and have full control over it. ○ PRIVATE PERMISSIONED: Completely Restricted. Only known and trusted users can join the blockchain. The administrator (trust-anchor) has control over users' data.
	To what extent do you AGREE or DISAGREE with the following statements?
Awareness2	My organisation is aware of BDIDM
Security	BDIDM satisfies the requirement of confidentiality
	BDIDM satisfies the requirement of integrity
	BDIDM satisfies the requirement of availability
Privacy	WAS NOT MEASURED UNINTENTIONALLY
Trialability	BDIDM is easy for the user to adapt
Complexity	BDIDM is easy for an organisation to implement
Observability	BDIDM is easy for an organisation to control and monitor
Integration	BDIDM system is ready enough to integrate the enterprise ecosystem
Compatibility	BDIDM system easily interoperate with other systems
Competences	There are Blockchain skills available in my organisation

IT infrastructure1	My organisation's current IT infrastructure is appropriated for BDIDM implementation
Standardisation	Blockchain is normalised and standardised enough
Technology Readiness	There are well-established rules and procedures to guide Blockchain implementation in organisations
SECTION C: ORGANISATION CONTEXT	
	To what extent do you AGREE or DISAGREE with the following statements?
Employees Linkage	Formal and informal employees networking are necessary for the adoption of BDIDM in my organisation
Presence Product Champion	Availability of product champions is necessary for the adoption of BDIDM in my organisation
Top management support	Top-management support in strategic planning for BDIDM is necessary for its adoption in my organisation
Leadership and Communication	Communication about BDIDM importance and role in an organisation is necessary for its adoption
Organisation Readiness	Organisational preparedness, including financial, is necessary for BDIDM adoption
Organisation Awareness	The level of knowledge about BDIDM is necessary for the adoption of BDIDM in organisations
SECTION D: ENVIRONMENT CONTEXT	
	To what extent do you AGREE or DISAGREE with the following statements?
Vendor Support	Availability of credible BDIDM vendors is necessary for the adoption of BDIDM in my organisation
Skill Labour	Availability of Blockchain skills is necessary for the adoption of BDIDM in my organisation
Consultants	The availability of Blockchain consultants is necessary for the adoption of BDIDM in my organisation
Industry Pressure	There is an industry pressure for BDIDM adoption in my organisation
Competition Intensity	There is a competitive pressure for BDIDM adoption in my organisation
Government Regulation	Adoption of BDIDM comply with government regulation on identity management
Compliance with Standards	Adoption of BDIDM comply with organisation standards on identity management
SECTION E: FINAL THOUGHT	
Adoption Indicator	Would you recommend Blockchain-based identity management to your organisation?
Barriers	What are your (main) reasons for NOT recommending BDIDM to your organisation? PLEASE SELECT ALL APPLIED.
Enablers	What are your (main) reasons for recommending BDIDM to your organisation? PLEASE SELECT ALL APPLIED.
BDIDM Type	If you were to, which type of BDIDM would you be likely to recommend to your company? ○ PUBLIC PERMISSIONLESS BDIDM: Not restricted. Anyone can join the blockchain and get their ID. Users self-manage their ID. Every user has full control over their ID and can use it wherever they wish to. ○ PUBLIC PERMISSIONED BDIDM (Federated Blockchain): Somewhat restricted. Some users can join the blockchain and get their IDs, and users self-manage their IDs. Every user has full control over their ID and can use it wherever they wish to. ○ PRIVATE PERMISSIONED BDIDM: Completely Restricted. Only known and trusted users can join the blockchain and get their IDs. The administrator (trust-anchor) has control over users' IDs (e.g., the administrator can block an ID if necessary).

Appendix 3: Ethics Approval

Faculty of Commerce

Private Bag X3, Rondebosch, 7701
2.26 Leslie Commerce Building, Upper Campus
Tel: +27 (0) 21 650 4375/ 5748 Fax: +27 (0) 21 650 4369
E-mail: jacques.rousseau@uct.ac.za
Internet: www.uct.ac.za

@Commerce UCT **UCT Commerce Faculty Office**

04/11/2020

Sarah Mulaji

Department of Information Systems

University of Cape Town

REF: REC 2020/11/003

Blockchain-based Distributed Identity Management in Organisations

We are pleased to inform you that your ethics application has been approved. Unless otherwise specified this ethical clearance is valid until 30-Nov-2021 .

Your clearance may be renewed upon application.

Please be aware that you need to notify the Ethics Committee immediately should any aspect of your study regarding the engagement with participants as approved in this application, change. This may include aspects such as changes to the research design, questionnaires, or choice of participants.

The ongoing ethical conduct throughout the duration of the study remains the responsibility of the principal investigator.

We wish you well for your research.

2020.11.04
14:25:45 +02'00'

Jacques Rousseau
Commerce Research Ethics Chair
University of Cape Town
Commerce Faculty Office
Room 2.26 | Leslie Commerce Building

Office Telephone: +27 (0)21 650 2695 / 4375
Office Fax: +27 (0)21 650 4369
E-mail: jacques.rousseau@uct.ac.za
Website: https://www.commerce.uct.ac.za/Pages/Ethics-in-Research

"Our Mission is to be an outstanding teaching and research university, educating for life and addressing the challenges facing our society."