Hindawi
Security and Communication Networks
Volume 2021, Article ID 9910078, 19 pages
https://doi.org/10.1155/2021/9910078

Review Article

The Practicality of Adopting Blockchain-Based Distributed Identity Management in Organisations: A Meta-Synthesis

Sarah S. M. Mulaji and Sumarie S. Roodt

Department of Information Systems, University of Cape Town, Rondebosch 7700, Cape Town, South Africa

Correspondence should be addressed to Sarah S. M. Mulaji; mljsar001@myuct.ac.za

Received 18 March 2021; Revised 24 July 2021; Accepted 25 October 2021; Published 28 November 2021

Academic Editor: Yinghui Zhang

Blockchain has become an irresistible disruptive technology with the potential to innovate businesses. Ignoring it may in itself result in a competitive disadvantage for organisations. Except for its original financial application of cryptocurrency, more applications are being proposed, the most common being supply chain management and e-voting systems. However, less focus is made on information and cybersecurity applications of blockchain, especially from the enterprise perspective. This paper addresses this knowledge gap by exploring blockchain as a use case for identity management in the context of an organisation. The paper gives a comprehensive background aiming at understanding the topic, including understanding whether claims made around it, especially blockchain's potential to address identity management challenges, are based on facts or just a result of hype. Meta-synthesis was used as a research methodology to summarise the 69 papers selected qualitatively from reputed academic sources. The general trend shows theoretical evidence supporting some of the claims made but not necessarily friendly to the enterprise context. The study reveals a promising but immature state of blockchain, consequently questioning whether adopting blockchain-based distributed identity management in organisations is fully practical. A research model called TOE-BDIDM is proposed to guide further investigation.

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" [1]. One of the fundamental steps in enforcing data integrity is safeguarding the digital system (such as a network, a website, a database, and an application) 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 [2]. For example, a Serianu report revealed that Africa has one of the highest cybercrimes and financial losses [3]. The IBM 2019 Cost of a Data Breach Study reported an increase in the average cost of a data breach in South Africa, by 12% from 2018 to 2019 [4].

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" [1]. Others claim that (iii) blockchain systems have "arguably no single point of failure vulnerability" [5] and that (iv) blockchain identities are privacy-preserving and (v) "give back to users their power over their data" [6]. Further claims suggest that (vi) centralised IDM systems are "subject to different problems and threats such as data breaches" [7], hence should (vii) evolve to possess distributed, disintermediated and secure capabilities [1]. Therefore, it was worthwhile to explore blockchain as a use case for IDM in organisations.

This study explores how practical adopting blockchain-based distributed identity management (BDIDM) is from the organisational perspective, providing a comprehensive background to understand the topic. This includes understanding whether claims about blockchain concerning IDM, especially blockchain potential to address IDM challenges, are based on facts or merely a result of hype. Because there is so much ambiguity around blockchain topics, "their true nature is often obscured by marketing and hype" [8]. Before reporting the review results, the following section will discuss the methodology followed to execute the research.

2. Methodology

This explorative study followed a "qualitative meta-aggregation and meta-summary" research methodology called meta-synthesis. The latter seeks to summarise and "distil information to draw conclusions" [9] 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 [10].

This study 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 [11]. 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 linear, typically analyses findings across quantitative studies "to identify statistically significant results" [9], and tends to prioritise objectivity over richness [10]. The predefined rules in this review were the review scope, data location (databases), search terms, selection criteria, exclusion criteria, and techniques and procedures of analysis and synthesis. The initial phase consisted of framing the review exercise, determining the scope of the review.

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" [10]. 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 the two represent the interrelationships between them (MT3: "enterprise perspective of BDIDM and implementation proposals" and MT4: "related theories").

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 and simplicity* when synthesising them.

Diversity in information sources was achieved by including unusual sources such as 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 such as 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" [10].

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" [10]. The remaining selection criteria were simply based on common sense.

The fairness of the results was ensured by assessing the quality of individual studies using the ten basic claims by Ngwenyama [12] 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" [10]. After all, the review adopted a centric approach that values both studies' inclusion and results' fairness. In addition, the review assessed the validity of the claims made about the topic using related theories.

The 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" [10].

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

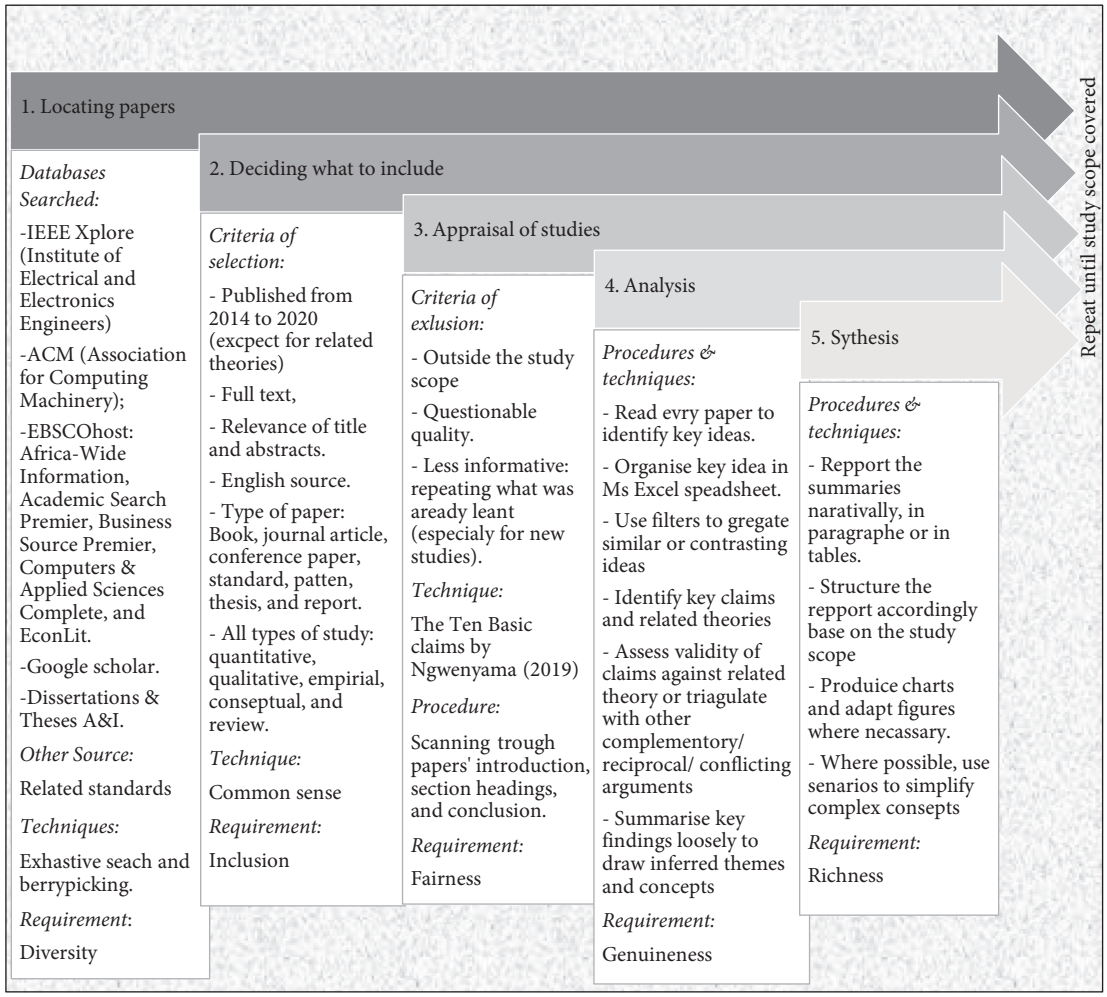

Figure 1: Summary of the five phases of the review exercise.

Table 1: List of search terms.

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

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 [10].

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 made of 32 conference papers (46.4%), 25 journal articles (36.2%), and 6 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.

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

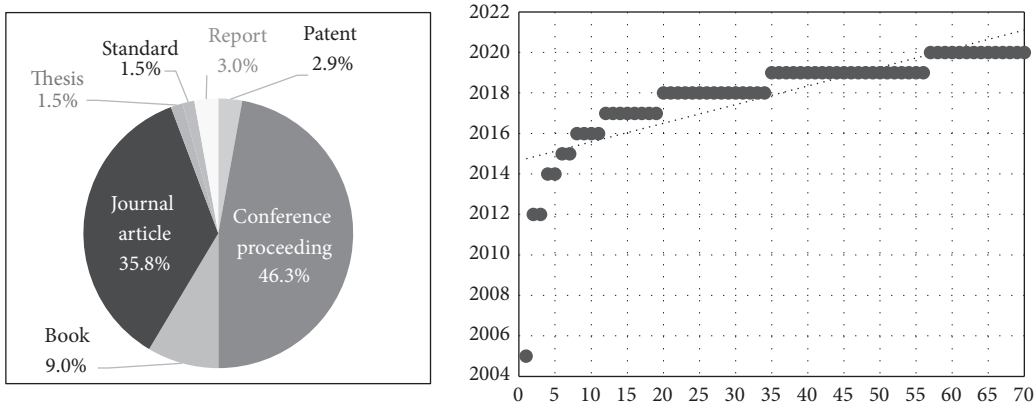

Figure 2: Description of the sample from the perspective of type and year of publication.

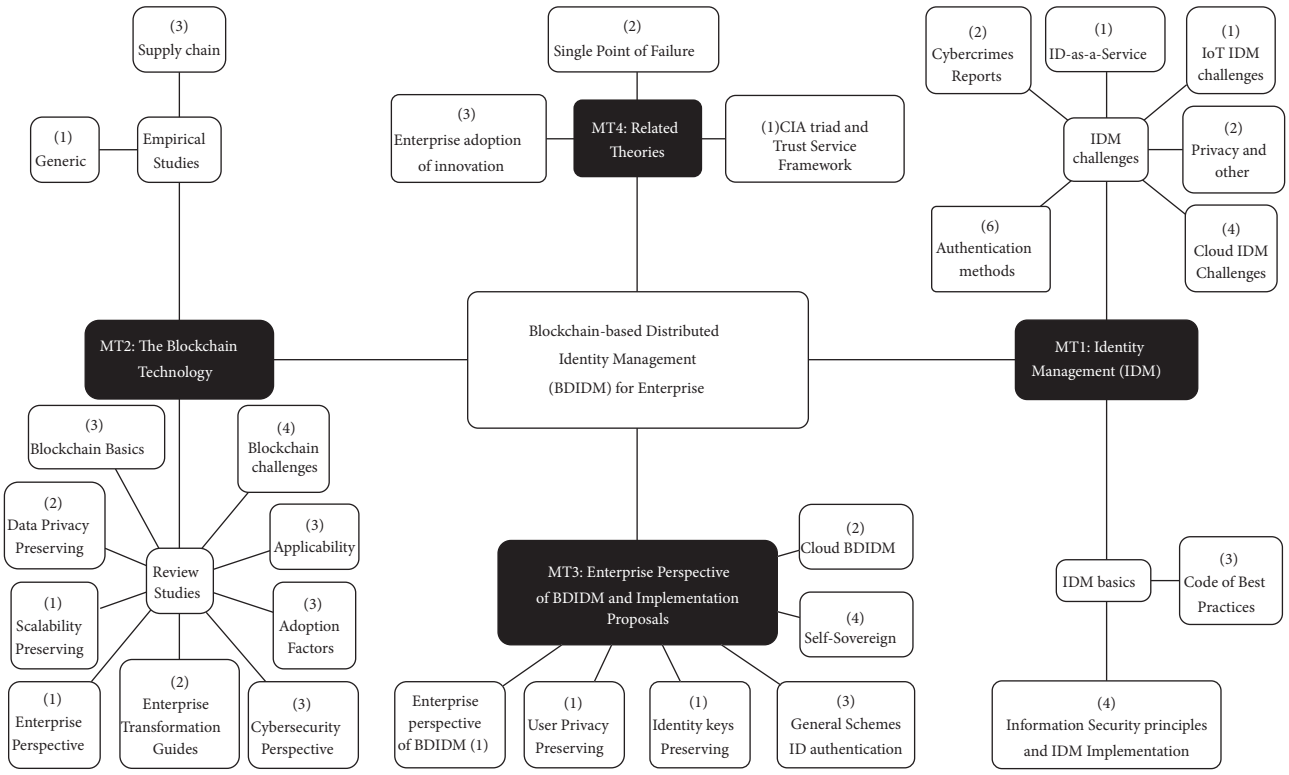

Figure 3: Thematical distribution of sources.

the 4 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 7 for "IDM basics" subthemes), 14 papers under MT3: "BDIDM implementation proposals" and "enterprise perspective of BDIDM," and 6 papers under MT4: "related theories."

3. Results and Discussion

This section reports the review findings narratively. The review is structured in such a way to cover the main themes within the review scope, as shown in Figure 3. MT1 relates to IDM fundamentals, IDM challenges that need to be addressed and the evolution of IDM models to address IDM challenges. MT2 concerns blockchain fundamentals, including 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 explains factors that impact BDIDM adoption in organisations based on the technology-organisation-environment theory.

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

3.1. 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 [13].

Technically, IDM consists of managing matters related to two fundamental information security 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, and so on. 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 (nonrepudiation or nondenial) [14].

> 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"
>
> Authorisation: "*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 [14]

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, e.g., a password, phone number, PIN, biometrics, etc.) and stores its relevant identity information on a dedicated component (generally a server) [2].

3.2. The Criticality of Addressing IDM Challenges in Organisations. IDM is a fundamental security control that mitigates security breaches in organisations [14]. 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."

3.2.1. Vulnerabilities in Authentication Methods. Authentication is a principle of information security 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 [14].

Unfortunately, every authentication method has known vulnerabilities and can be compromised. Knowledge-based methods like passwords and PIN are vulnerable to guessing attacks such as dictionary, rainbow table, bruteforce, and so on [14]. Moreover, users may experience difficulties in matching their passwords to different accounts [15]. 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-positive and false-negative rates [16, 17]. Soft biometrics methods such as signatures and typing patterns, as well as location-based methods such as the Global Positioning System (GPS) and Indoor Positioning System (IPS), are only secondary to continuously verifying an authenticated user [18].

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" [14]. Therefore, codes of best practices in information security, including the ISO/EIC and NIST, recommend the use of multifactor authentication (MFA) to establish "strong authentication and identity verification" [19, 20]. 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 [21, 22].

3.2.2. 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 [22]. 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" [23] would mitigate the SPOF vulnerability and achieve reliability and resilience in digital systems [24]. Redundancy involves having a duplicate copy of the database on every node, generally known as distribution [25]. That is why distributed systems, such as blockchains, have "arguably no single point of failure vulnerability" [5].

In Figure 4, 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 [25]. The failure of the server knocks the whole system down [22]. 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 [5].

3.2.3. Balance between Security and Privacy. The ongoing data breaches in organisations indicate the need to ensure effective identity and access management systems [26]. 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 "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 such as POPIA in South Africa. Users, of course, "want good services offered in convenient ways" yet are very "concerned about infringements to their privacy" [27].

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" [28]. 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" [2]. This issue verifies the theory of "the CIA triad," an acronym for three fundamental objectives of information security: *confidentiality*, *integrity*, and *availability*.

Whitman and Mattord indicate that the CIA triad "has been the standard for computer security in both industry and government since the mainframe development" [14], 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 unauthorised access to information; integrity prevents unauthorised modification of information; and availability ensures the information is always available to authorised users [14]. However, another underlying requirement for a digital system is privacy. Privacy prevents unauthorised access to the personal data of employees, clients, partners, and so on. Figure 5 illustrates a typical application of this extended CIA as the Trust Service Framework (TSF), developed by Romney et al. [29] 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.

3.2.4. 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 [14]. Users have been reusing the same credentials on different services, creating redundant security data [30]. 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.

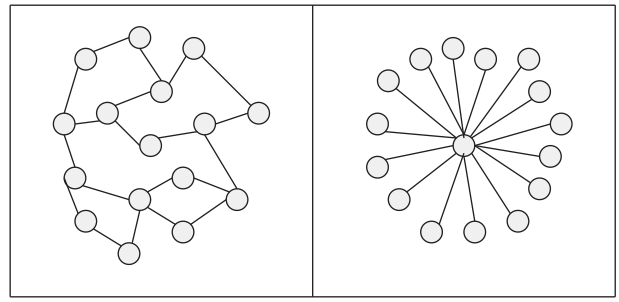

Figure 4: Distributed versus centralised system architecture (adapted from [25]).

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.

3.2.5. "Secure Cloud" and "Secure IoT". Initially, IDM systems were used to identify a living individual in a digital system and involved authenticating them as a legitimate user of the system [2]. Today, IDM systems need to identify and authenticate not only individuals but also "things" such as software, smartphone, robot, automobile, appliances, entertainment devices, and so on—hence the origin of the so-called IoT, an acronym for internet of things [31]. 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 [14].

Furthermore, secure and reliable IDM appears to be "the greatest challenge facing cloud computing today" [32]. Although "accountability is the main construct and key enabler of trust" in the cloud [33], "secure and reliable management of identities" is proven "the greatest challenges facing cloud computing today" [34]. Effective IDM in the cloud is a "key area of cloud security" and is vital for its wide adoption [35, 36], Still, traditional cloud-based identity and access control systems follow a centralised approach, where a cloud server acts as the central authority controlling access to data in the cloud [37].

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

3.3. 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 centralised 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 [2]. Figure 6 illustrates the contrast between the two approaches.

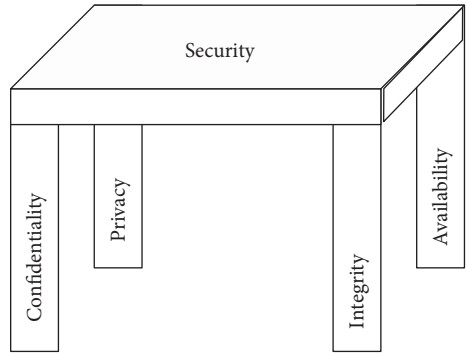

Figure 5: The CIA triad and the TSF.

3.3.1. Centralised 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" [7]. As a result, "users are forced to rely on a different central service to manage their identity data in each different domain" [2]. 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)" [2]. Centralised IDM systems use protocols such as RADIUS and Kerberos, providing authentication of both individuals and applications on a dedicated server [38].

3.3.2. 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, such as OKTA or AWS-IAM, providing authentication of both individuals and applications on a dedicated server in the cloud [7, 39].

3.3.3. Federated IDM. Federated IDM is a model of trust that helps mitigate partially the problems posed by centralised 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" [38]. When signing on a trusted third-party system, "the user is redirected for authentication and user identity data retrieval to his home *identity provider*" [7]. 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 [14]. 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, SAMUAL, and Auth [40].

3.3.4. User-Centric 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" [2]. 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 [27].

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)." However, 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" [7].

3.3.5. Self-Sovereign Identity (SSI). A typical user-centric IDM uses blockchain to obtain SSI systems [41]. In this model, the decentralized 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" [42]. That is why a growing tendency portraits SSI as the most "privacy-respectful solution" for IDM systems [7]. Identity data is stored on the user side, technically on their individual block, using a software wallet installed on their device (like a smartphone) [43]. "Users can register, retrieve and even revoke the data if they do not want to use them anymore" [5].

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

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

3.4. The Blockchain Technology. Blockchain is a constantly growing distributed record of updates about a specific matter among a group of participants. A consensus protocol

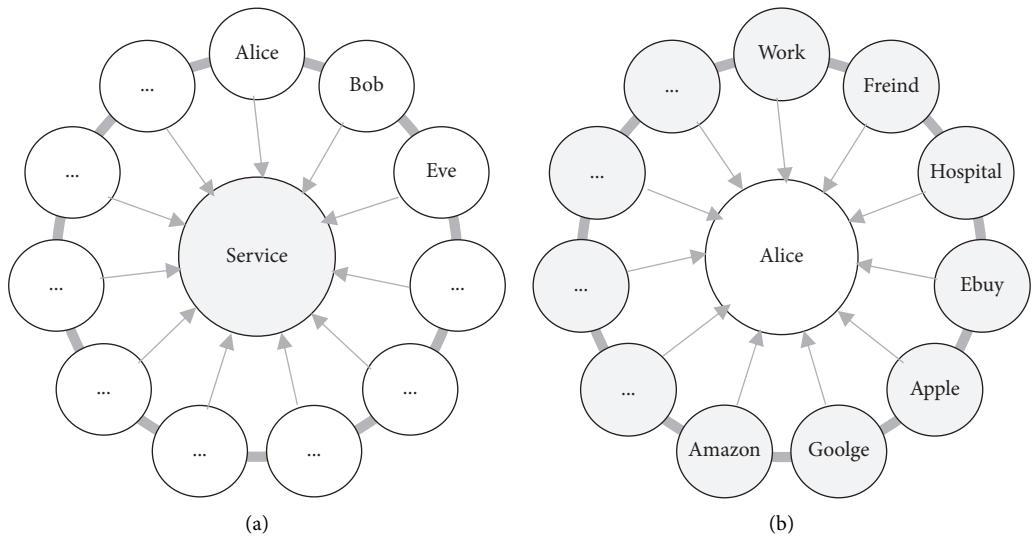

Figure 6: Traditional centralised IDM (a) versus self-sovereign identity (b) models (adapted from [2]).

regulates interactions among participants, and cryptographic technologies, namely digital signature and hash algorithm, maintain security [44, 45]. 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 [46, 47].

3.4.1. Enterprise Blockchain (EB). The concept of EB refers to a "permissioned blockchain utilized by any organisation" [48]. However, ambiguities on the applicability of EB in the real world are 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" [49]. 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 [47] 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.

3.4.2. Promoting and Constraining Factors ofEB. There are eight important architectural properties of blockchain, paired in a mutual influence relation, that could promote its adoption: decentralisation and disintermediation, programmability and automation, transparency and auditability, and immutability and verifiability [50]. 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.

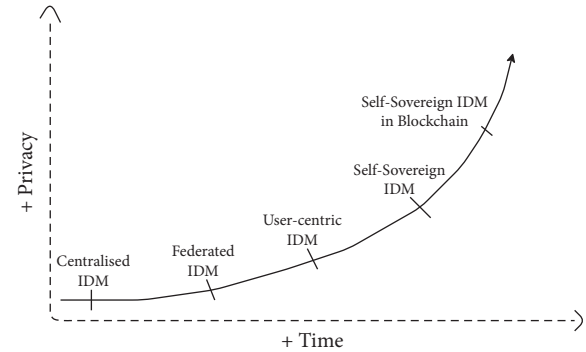

Figure 7: IDM models evolvement over time from the user privacy perspective (adapted from [7]).

Blockchain is a relatively new technology that is still suffering from immaturity [49]. Table 4 discusses the fundamental challenges ahead of its implementation that might prevent or delay its adoption in organisations.

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

3.5. The Practicality of Adopting BDIDM in Organisations. This subsection 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.

3.5.1. The Practicality of the Concept. The following scenario set 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,

Table 2: Blockchain implementation types.

Blockchain implementation					
Consensus protocol	Raft consensus	Prof. of authority (PoA)	Federated consensus	Prof of work (PoW)	Prof of stake (PoS)
Who can join/ validator trust	Private/permissioned	Public/permissioned		Public/permissionless	
Description	"access authorization does not entail validation permissions, which require additional authorization rights given to several nodes." Only trustful nodes enforce consensus.	"only authenticated and predefined users can read and write transactions. All nodes participate in the finding of the consensus. Identifiable nodes determine consensus mechanisms.".		"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."	
Application	Enterprise projects (Hyperledger)	Organisational consortia (Ripple, R3)		Cryptocurrencies (Bitcoin)	
References	[46, 47]				

Table 3: Blockchain promoting factors.

Blockchain features and business impacts	
Decentralization and disintermediation	Blockchain eliminates system dependencies and intermediaries [1]. It enables direct interactions between participants without the need for a trusted third party [50, 51].
Programmability and automation.	Smart contracts allow for automated execution of predefined codes "once certain conditions have been met," though arbitrary code may increase bugs [50]. Automation "simplifies complex business processes by alleviating the need for manual interventions" [49].
Transparency and auditability	Each user of the blockchain can track how blocks have been added over time [52]. However, a permissioned blockchain might reduce transparency due to the privacy requirement [53].
Immutability and verifiability	Blockchain keeps temper-evident historical records of all transactions happening on the network [49]. "The information stored in the blocks cannot be changed unless an attacker can gather more than 51% of the computational power network" [52, 54].
Integrity, authentication of origin, and trust	Cryptographic methods ensure that information is protected from unauthorised modifications, improving trust [52, 53].

national identification number, age, e-mail 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" [1, 42]. 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 [6].

3.5.2. 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 decentralised and distributed [62]. Decentralisation refers to the removal of the IDM central authority (server). In contrast, distribution refers to utilising the exact copy of a user's ID across all components of the IDM system (redundancy) [2].

Table 4: Blockchain constraining factors.

	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 [49]. Recurrent updates make the blockchain system "highly volatile" [55].
Technical integration challenges	Due to its decentralised architecture, blockchain may make it difficult to connect with legacy systems [49]. A poorly designed blockchain can result in a system incompatible with existing systems, such as "a fine-grained identity" [55] and role-based access control [56].
Scalability and performance	Blockchain requires a careful design to "ensure sufficient scalability without sacrificing decentralisation" [1]. Scalability is generally measured in throughput, latency, bootstrap time, storage, cost of confirmed transactions, fairness, and network utilization [8].
Security	It is possible to breach the security of a blockchain "when a "miner" controls more than 51% of the computing power" [54, 57]. Although this is still thought very difficult to achieve, it may not be impossible with quantum computing [1, 58].
Skill shortage	"Blockchain-focused technical skills are not yet taught in standard higher education curricula" [59]. As a result, the industry is suffering from a deficit of expertise. Meanwhile, the demand for blockchain skills is growing [49, 59].
Complexity	Blockchain is considered both "user and developer unfriendly." It is thought complex to implement and difficult for a user to adapt [60].
	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." Its upfront implementation cost is high, as it includes new infrastructure and a highly skilled team, which rather negatively impact existing revenues [49]
Governance	"The governance of a blockchain concerning updating its fundamental rules is problematic" [50]. "The whole network relies on a consensus mechanism" that involves all the nodes, "which can be any device" [61]. Therefore, there are issues of accountability and management [56].
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" [49, 59].
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" [49].
Awareness	The widespread adoption of blockchain is also potentially restricted by the lack of adequate knowledge and awareness [56].

> 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" [2].

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 notarise 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 "inquires into the identity of the subject" [5]. 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 [43]. 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" [7].

The principles of SSI include existence, control, access, transparency, persistence, portability, interoperability, consent, minimalisation, and protection [2]. 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" [2]. 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 [14]. 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" [54, 57]. This cyberattack on blockchains may still be though difficult to achieve but may not be impossible with quantum computing [58, 60].

3.5.3. The Practicality of the Ideal Blockchain Implementation . Figure 9 shows that public permissionless blockchains, on the one hand, tend to be decentralized, transparent, and scalable but inefficient in computing power and, thus, are

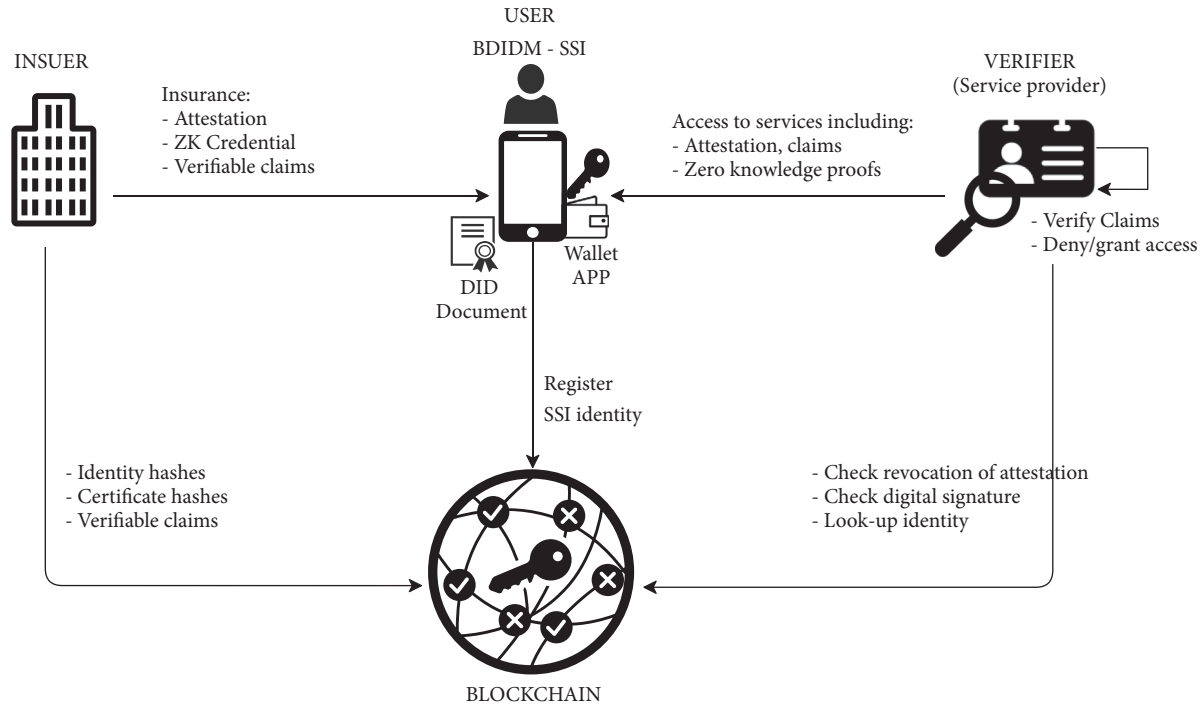

Figure 8: SSI model (adapted from [7]).

slow. On the other hand, private permissioned blockchains tend to be more centralised, less transparent, and not scalable but efficient in computation power consumption and, 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 centralised" [2].

Public permissioned blockchains, also known as federated blockchains, are more balanced versions of blockchains [63]. They tend to fit the concept of federated IDM discussed earlier and are claimed to be more decentralised, scalable, and efficient [57] and ensure "privacy protection and high transparency" [62]. 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 [7].

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 [37].

Wüst and Gervais [53] 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 [14], 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 recommends 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)" [64]. 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

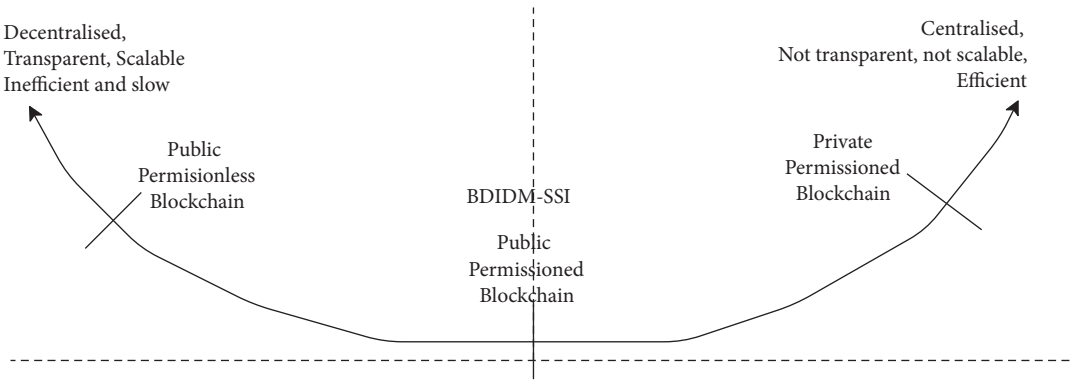

Figure 9: Balancing decentralisation and transparency to achieve efficient blockchains.

significantly expensive," which is why it is claimed to create a trusted system in an untrusted environment [1].

3.5.4. The Practicality of BDIDM 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 [51]. 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" [6]. "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" [2]. 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" [65].

However, "reluctance to adopt disruptive technologies may be a significant competitive disadvantage for an organisation, whereas proactive planning can be a significant advantage" [49]. 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" [1].

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. Di Francesco Maesa and 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 centralised solutions" and 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" [2].

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 [66]. 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 [5]. Since the IoT relies on the cloud, the "current centralised 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 [31].

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" [2]. 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" [49].

Still, an objective viewpoint would add that more empirical evidence is needed to prove the prevailing argument, since there is more that could impact the likelihood of an organisation to adopt such innovation. The literature suggests some theories that could holistically explain the adoption phenomenon. These theoretical considerations are key in anticipating factors that might predict BDIDM adoption, in this way reconcile views around whether to adopt this innovation in organisations while providinglenses that could be used to further investigate thisphenomenon.

3.6. Theoretical Considerations about the Adoption of BDIDM in Organisation. This subsection analyses how related

theories would shape the adoption of BDIDM in organisations. The section identifies the technology-organisation-environment (TOE) theory as more suitable for explaining this matter than other competing theories. The section ends by proposing a revised version of the TOE theoretical framework, called TOE-BDIDM, as a research model for future empirical studies.

3.6.1. 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 the studies of Kamble et al. [67] and Queiroz and Fosso Wamba [68] that were based on individual blockchain adoption, this study considers the enterprise perspective of blockchain adoption like those by Clohessy and Acton [69] and Karamchandani et al. [48]. 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 and 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 [70].

Unlike some studies limiting the framework to the organisational element only, considering it "the most significant determinant of IT innovation adoption in organisations" [69], this study considers the entire TOE framework. Karamchandani et al. [48] 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" [70].

3.6.2. 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 [70]. Existing technologies such as centralised access control may play a key role in adopting BDIDM as they may not be compatible with a distributed architecture [55]. 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. Baker adds that the innovation's characteristics, that is, the extent of the change it brings, also impact its adoption decision-making. 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 [70]. Blockchain tends to shift the security paradigm by assuming "the presence of adversaries in the network" [1]. 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 information security perspective, Hameed and Arachchilage [71] 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 adopt/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" [72], which includes the availability of skills, consultants, vendors, and so on. However, Baker [70] identifies these items under external environment instead.

3.6.3. 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 decentralised organisational structure may be suited for the BDIDM adoption phase. Those with formal reporting relationships, centralised decision-making, and clearly defined roles for employees may be the best in the implementation phase [70].

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 [70]. Regarding BDIDM, since organisations tend to be hostile to privacy, "top management support and organisational readiness are enablers for the adoption of Blockchain" [69].

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 [70]. Instead,

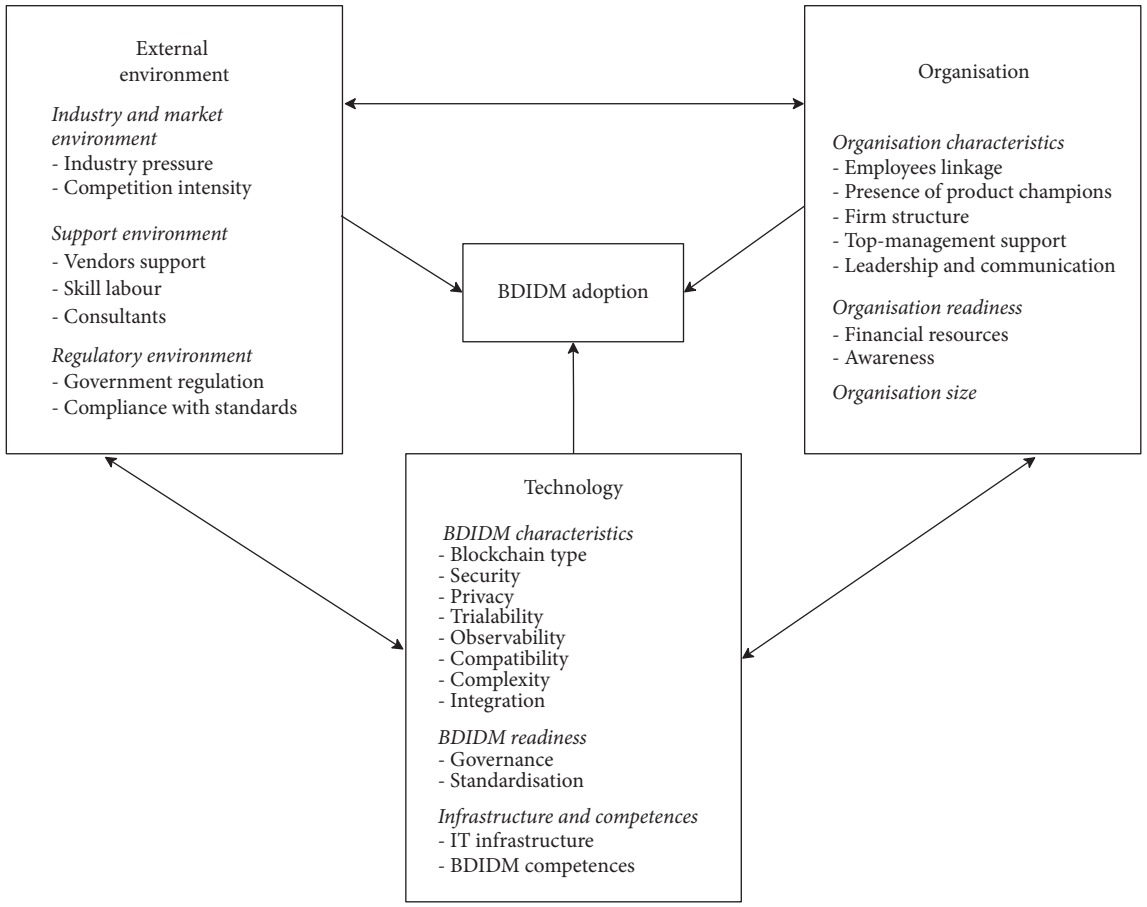

Figure 10: TOE-BDIDM.

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 [49], 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 [69]. Besides, cultural adaption, awareness, and reluctance to change may also impact the adoption of BDIDM [56].

3.6.4. 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 [70].

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 [20] and NIST [19]), and cyber-threat landscape could impact BDIDM adoption in organisations [22, 73]. However, blockchain still lacks firm regulatory guidelines and policies for standardisation [49, 59].

3.6.5. The TOE-BDIDM Research Model. Figure 10 illustrates TOE-BDIDM, the proposed research model to empirically investigate the TOE factors impacting 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 [70]. The revision aimed to adapt the TOE model to the information security and blockchain contexts. For example, the items "readiness" and "awareness" were added due to the relative newness of the blockchain [49, 56]. Governance and standardisation of the blockchain would also impact the decision to adopt BDIDM in organisations [50]. The literature shaped additional 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.

4. Conclusions

This section synthesises the findings considering the study's objectives and scope introduced earlier. The section also

highlights several knowledge gaps identified in the literature as hints for further research and ends by giving key study's limitations.

This study sought to explore the literature to provide background on the BDIDM as a use case of blockchain. The aim was to understand the topic, mostly how practical the adoption of BDIDM was from an organisational perspective. The study tacitly demonstrated whether the claims made about blockchain, including its potential to address IDM challenges in organisations, were factual. Moreover, the study implicitly showed whether BDIDM was as disruptive for organisations (compared to traditional IDM systems) as assumed.

4.1. Summary of Findings. The main findings could be synthesized as follows:

First, IDM consists of managing matters related to two fundamental information security 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, 5 business-promoting factors linked to its features: (i) decentralisation and disintermediation, (ii) programmability and automation, (iii) transparency and auditability, (iv) immutability and verifiability, and (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 decentralized and disintermediated 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 follows 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. Adopting BDIDM-SSI would eliminate the need for organisations to host personal identifiable information on their servers, and in this way, a data breach can be mitigated when the server is compromised. Supporters see the potential of blockchain to mitigate other IDM challenges, including cost-saving on the daily IDM maintenance due to the SSI's identity self-management feature. 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 such as 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 study appeared to have some theoretical foundation. This verifies that claims about blockchain, including its potential to address IDM challenges in organisations, are factual rather than just a result of hype.

Therefore, one could conclude 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 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 such as IDM challenges. Hence, the proposed TOE-BDIDM research model is suggested for further studies.

4.2. Gaps in the Literature and Future Research. 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 [47, 49] 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.

Second, 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.

Third, 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.

Last, of the empirical studies on blockchain retrieved, none was about blockchain-based identity 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 [69], while others used quantitative methods with different theories [68].

4.3. Limitations. This literature review is not perfect. The principal limitation was that not all potential papers were included in the sample. First, 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. There 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.

This literature review may not, on its own, be sufficient to make a case for BDIDM adoption in organisations. As far as its objective is concerned, it gives the background to understand the topic while inspiring further empirical investigations.

Data Availability

This research used secondary data: journal articles, conference papers, books, reports, patents, and standards. These are listed in the reference section, and most of them are accessible on common academic databases, including EBSCOhost and Google Scholar.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors would like to acknowledge Professor Michael Kyobe, Department of Information Systems at the University of Cape Town, for his guidance at the earlier stage of the drafting of this work. The authors also appreciate their families and friends' support during the drafting process.

References

[1] S. Shetty, C. A. Kamhoua, and L. L. Njilla, *Blockchain for Distributed Systems Security*, John Wiley & Sons, Hoboken, New Jersey, United States, 2019.

[2] D. Di Francesco Maesa and P. Mori, "Blockchain 3.0 applications survey," *Journal of Parallel and Distributed Computing*, vol. 138, pp. 99–114, 2020.

[3] P. Musuva-Kigen, F. Mueni, and D. Ndegwa, *Africa Cyber Security Report 2016*, Serianu Cyber Threat Intelligence Team, Nairobi, Kenya, 2016.

[4] IBM-Security, "IBM: cost of a data breach report," *Computer Fraud & Security*, vol. 2019, no. 8, p. 4, 2019.

[5] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[6] M. Kuperberg, "Blockchain-based identity management: a survey from the enterprise and ecosystem perspective," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1008–1027, 2019.

[7] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: review and challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019.

[8] J. Kolb, M. AbdelBaky, R. H. Katz, and D. E. Culler, "Core concepts, challenges, and future directions in blockchain," *ACM Computing Surveys*, vol. 53, no. 1, pp. 1–39, 2020.

[9] D. Finfgeld-Connett, *A Guide to Qualitative Meta-Synthesis*, Routledge, New York, NY, 2018.

[10] D. Walsh and S. Downe, "Meta-synthesis method for qualitative research: a literature review," *Journal of Advanced Nursing*, vol. 50, no. 2, pp. 204–211, 2005.

[11] G. Oosterwyk, I. Brown, and S. Geeling, "A synthesis of literature review guidelines from information systems journals," *Proceedings of 4th International Conference on the*, vol. 12, pp. 250–260, 2019.

[12] O. Ngwenyama, "The ten basic claims of information systems research: an approach to interrogating validity claims in scientific argumentation," *SSRN Electronic Journal*, pp. 1–40, 2019.

[13] D. Chakravarty and T. Deshpande, "Blockchain-enhanced identities for secure interaction," in *Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, pp. 1–4, IEEE, Crystal City, VA, USA, May 2018.

[14] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, Cengage Learning, Boston, Massachusetts, US, 2018.

[15] K. Marky, P. Mayer, N. Gerber, and V. Zimmermann, "Assistance in daily password generation tasks," in *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers*, pp. 786–793, Singapore, Singapore, October 2018.

[16] M. A. Kiran, P. Yogeshwari, K. V. Bhavani, and T. Ramya, "Biometric authentication: a holistic review," in *Proceedings of the 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)*, pp. 428–433, IEEE, Palladam, India, August 2018.

[17] T. Seitz, F. Mathis, and H. Hussmann, "The bird is the word: a usability evaluation of emojis inside text passwords," in *Proceedings of the 29th Australian Conference on Computer-Human Interaction*, pp. 10–20, Brisbane, Queensland, Australia, November 2017.

[18] L. Xiaofeng, Z. Shengfei, and Y. Shengwei, "Continuous authentication by free-text keystroke based on CNN plus RNN," *Procedia computer science*, vol. 147, pp. 314–318, 2019.

[19] W. A. Hufstetler, M. J. H. Ramos, and S. Wang, "Nfc unlock: secure two-factor computer authentication using nfc," in *Proceedings of the 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, pp. 507–510, IEEE, Orlando, FL, USA, October 2017.

[20] *South African National Standard: Information Technology — Security Techniques — Code of Practice for Information Security Controls*, ISO/IEC, Switzerland, 2014.

[21] S. Pranata and H. T. Nugroho, "2FYSH: two-factor authentication you should have for password replacement," *Telkomnika*, vol. 17, no. 2, pp. 693–702, 2019.

[22] Y. Liu, G. Sun, and S. Schuckers, "Enabling secure and privacy preserving identity management via smart contract," in *Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–8, IEEE, Washington, D.C, USA, June 2019.

[23] T. G. Rauscher, "Raid system with multiple controllers and proof against any single point of failure," Google Patents, 2005.

[24] B. Feng, C. Huang, and X. Gong, "Distributed storage method, apparatus, and system for reducing a data loss that may result from a single-point failure," Google Patents, 2014.

[25] D. Dresher, *Blockchain Basics*, Apress, Frankfurt, 2017.

[26] E. Karanja and M. A. Rosso, "The chief information security officer: an exploratory study," *Journal of International Technology and Information Management*, vol. 26, no. 2, pp. 23–47, 2017.

[27] J. Breuer, H. Ranaivoson, U. Buchinger, and P. Ballon, "Who manages the manager? Identity management and user ownership in the age of data," in *Proceedings of the 2015 13th Annual Conference on Privacy, Security and Trust (PST)*, pp. 22–27, IEEE, Izmir, Turkey, July 2015.

[28] D. Baars, *Towards Self-Sovereign Identity Using Blockchain Technology*, University of Twente, Enschede, Netherlands, 2016.

[29] M. Romney, P. Steinbart, J. Mula, R. McNamara, and T. Tonkin, *Accounting Information Systems Australasian Edition*, Pearson Higher Education AU, Australia, 2012.

[30] A.-S. Shehu, A. Pinto, and M. E. Correia, "Privacy preservation and mandate representation in identity management systems," in *Proceedings of the 2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1–6, IEEE, Coimbra, Portugal, June 2019.

[31] X. Zhu and Y. Badr, "A survey on blockchain-based identity management systems for the Internet of Things," in *Proceedings of the 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)*, pp. 1568–1573, IEEE, Halifax, NS, Canada, July 2018.

[32] R. Charanya and M. Aramudhan, "Survey on access control issues in cloud computing," in *Proceedings of the 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, pp. 1–4, IEEE, Pudukkottai, India, February 2016.

[33] J. K. Mwenya and I. Brown, "Cloud privacy and security issues beyond technology: championing the cause of accountability," in *Proceedings of the The 30th Australiasian Conference on Information Systems (ACIS)*, Perth, Western Australia, December 2019.

[34] K. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha, "WiP: a novel blockchain-based trust model for cloud identity management," in *Proceedings of the 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)*, pp. 724–729, IEEE, Athens, August 2018.

[35] X. Ma, "Managing Identities in Cloud Computing Environments," in *Proceedings of the 2015 2nd International Conference on Information Science and Control Engineering*, pp. 290–292, IEEE, Shanghai, China, April 2015.

[36] F. F. Moghaddam, P. Wieder, and R. Yahyapour, "A policy-based identity management schema for managing accesses in clouds," in *Proceedings of the 2017 8th International Conference on the Network of the Future (NOF)*, pp. 91–98, IEEE, London, UK, November 2017.

[37] N. Sohrabi, X. Yi, Z. Tari, and I. Khalil, "BACC: blockchain-based access control for cloud data," in *Proceedings of the Australasian Computer Science Week Multiconference*, pp. 1–10, Melbourne, VIC, Australia, February 2020.

[38] D. Alexander, A. Finch, D. Sutton, and A. Taylor, *Information Security Management Principles*, Third Edition ed. edition, 2020.

[39] N. Mpofu and W. J. van Staden, "Evaluating the severity of trust to identity-management-as-a-service," in *Proceedings of the 2017 Information Security for South Africa (ISSA)*, pp. 83–89, IEEE, 54 on Bath Hotel, Rosebank, Johannesburg, South Africa, August 2017.

[40] S. Michael and Z. J. Anna, "An identity provider as a service platform for the edugain research and education community," in *Proceedings of the 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pp. 739-740, IEEE, Washington, DC, USA, April 2019.

[41] M. A. Bouras, Q. Lu, F. Zhang, Y. Wan, T. Zhang, and H. Ning, "Distributed ledger technology for eHealth identity privacy: state of the art and future perspective," *Sensors*, vol. 20, no. 2, p. 483, 2020.

[42] A. Grüner, A. Mühle, and C. Meinel, "An integration architecture to enable service providers for self-sovereign identity," in *Proceedings of the 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA)*, pp. 1–5, IEEE, Cambridge, MA, USA, September 2019.

[43] A. R. Thota, P. Upadhyay, S. Kulkarni, P. Selvam, and B. Viswanathan, "Software wallet based secure participation in hyperledger fabric networks," in *Proceedings of the 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pp. 1–6, IEEE, Bengaluru, India, January 2020.

[44] H. Kim, S.-H. Kim, J. Y. Hwang, and C. Seo, "Efficient privacy-preserving machine learning for blockchain network," *IEEE Access*, vol. 7, pp. 136481–136495, 2019.

[45] R. Post, K. Smit, and M. Zoet, "Identifying factors affecting blockchain technology diffusion," in *Proceedings of the Americas Conference on Information Systems (AMCIS 2018)*, New Orleans LA, USA, August 2018.

[46] E. Politou, F. Casino, E. Alepis, and C. Patsakis, "Blockchain mutability: challenges and proposed solutions," *IEEE Transactions on Emerging Topics in Computing*, p. 1, 2019.

[47] O. Labazova, "Towards a framework for evaluation of blockchain implementations," in *Proceedings of the International Conference on Information Systems*, ICIS, Munich, Germany, December 2019.

[48] A. Karamchandani, S. K. Srivastava, and R. K. Srivastava, "Perception-based model for analyzing the impact of enterprise blockchain adoption on SCM in the Indian service industry," *International Journal of Information Management*, vol. 52, Article ID 102019, 2020.

[49] M. Demir, O. Turetken, and A. Mashatan, "An enterprise transformation guide for the inevitable blockchain disruption," *Computer*, vol. 53, no. 6, pp. 34–43, 2020.

[50] B.-J. Butijn, D. A. Tamburri, and W.-J. v. d. Heuvel, "Blockchains," *ACM Computing Surveys*, vol. 53, no. 3, pp. 1–37, 2020.

[51] P. Helebrandt, M. Bellus, M. Ries, I. Kotuliak, and V. Khilenko, "Blockchain adoption for monitoring and management of enterprise networks," in *Proceedings of the 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 1221–1225, IEEE, UBC, Vancouver , BC , Canada, 2018.

[52] N. El Madhoun, J. Hatin, and E. Bertin, "Going beyond the blockchain hype: in which cases are blockchains useful for it applications?" in *Proceedings of the 2019 3rd Cyber Security in Networking Conference (CSNet)*, pp. 21–27, IEEE, November 2019.

[53] K. Wüst and A. Gervais, "Do you need a blockchain?" in *Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 45–54, IEEE, Zug, Switzerland, June 2018.

[54] M. Ahmed, I. Elahi, M. Abrar, U. Aslam, I. Khalid, and M. A. Habib, "Understanding blockchain: platforms, applications and implementation challenges," in *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems*, pp. 1–8, Paris France, July 2019.

[55] A. Marsalek, C. Kollmann, T. Zefferer, and P. Teufl, "Unleashing the full potential of blockchain technology for security-sensitive business applications," in *Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 394–402, IEEE, Seoul, South Korea, May 2019.

[56] N. Upadhyay, "Demystifying blockchain: a critical analysis of challenges, applications and opportunities," *International Journal of Information Management*, vol. 54, Article ID 102120, 2020.

[57] Q. T. Thai, J.-C. Yim, and S.-M. Kim, "A scalable semi-permissionless blockchain framework," in *Proceedings of the 2019 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 990–995, IEEE, Jeju Island, South Korea, October 2019.

[58] E. Fernando, "Essential blockchain technology adoption factors in pharmaceutical industry," in *Proceedings of the 2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, pp. 523–526, IEEE, Yogyakarta, Indonesia, November 2019.

[59] P. T. Duy, D. T. T. Hien, D. H. Hien, and V.-H. Pham, "A survey on opportunities and challenges of Blockchain technology adoption for revolutionary innovation," in *Proceedings of the Ninth International Symposium on Information and Communication Technology*, pp. 200–207, Danang City, Viet Nam, December 2018.

[60] P. G. Lopez, A. Montresor, and A. Datta, "Please, do not decentralize the Internet with (permissionless) blockchains," in *Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems*, pp. 1901–1911, IEEE, Dallas, TX, USA, July 2019.

[61] Z. Cui, F. Xue, S. Zhang et al., "A hybrid BlockChain-based identity authentication scheme for multi-WSN," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241–251, 2020.

[62] T. Mitani and A. Otsuka, "Traceability in permissioned blockchain," *IEEE Access*, vol. 8, pp. 21573–21588, 2020.

[63] F. Buccafurri, G. Lax, A. Russo, and G. Zunino, "Integrating digital identity and blockchain," in *Proceedings of the OTM Confederated International Conferences on the Move to Meaningful Internet Systems*, pp. 568–585, Springer, Valletta, Malta, October 2018.

[64] V. Stafford, "Zero Trust Architecture," *NIST Special Publication*, vol. 800, p. 207, 2020.

[65] A. Rot and B. Blaicke, "Blockchain's future role in cybersecurity. analysis of defensive and offensive potential leveraging blockchain-based platforms," in *Proceedings of the 2019 9th International Conference on Advanced Computer Information Technologies (ACIT)*, pp. 447–451, IEEE, Ceske Budejovice, Czech Republic, June 2019.

[66] G. Wolfond, "A blockchain ecosystem for digital identity: improving service delivery in Canada's public and private sectors," *Technology Innovation Management Review*, vol. 7, no. 10, 2017.

[67] S. Kamble, A. Gunasekaran, and H. Arha, "Understanding the Blockchain technology adoption in supply chains-Indian context," *International Journal of Production Research*, vol. 57, no. 7, pp. 2009–2033, 2019.

[68] M. M. Queiroz and S. Fosso Wamba, "Blockchain adoption challenges in supply chain: an empirical investigation of the main drivers in India and the USA," *International Journal of Information Management*, vol. 46, pp. 70–82, 2019.

[69] T. Clohessy and T. Acton, "Investigating the influence of organizational factors on blockchain adoption: an innovation theory perspective," *Industrial Management & Data Systems*, vol. 119, no. 7, pp. 1457–1491, 2019.

[70] J. Baker, "The technology-organization-environment framework," *Information Systems Theory*, vol. 28, pp. 231–245, 2012.

[71] M. A. Hameed and N. A. G. Arachchilage, "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, Pennsylvania, United States, 2020.

[72] H. O. Awa, O. Ukoha, and B. C. Emecheta, "Using T-O-E theoretical framework to study the adoption of ERP solution," *Cogent Business & Management*, vol. 3, no. 1, Article ID 1196571, 2016.

[73] P. Grassi, *Digital Identity Guidelines: Enrollment and Identity Proofing*, National Institute of Standards and Technology, Gaithersburg, MD, US, 2017.