Al-Muthanna Journal of Administrative and Economic Sciences

PRINT ISSN: 2226-1419 - ONLINE ISSN: 2572-5386

Volume 16 | Issue 1 Article 11

2026-03-31

Blockchain Technology as a Tool to Enhance Information Security Elements in the Government Organizations Sector: An Exploratory Study in the Nineveh Governorate Traffic Directorate

Saif Khalid Zakaria

Department of Management Information Systems, College of Administration and Economics, University of Mosul, Mosul, Iraq, saif_khalid@uomosul.edu.iq

ENGLISH ARTICLE

Blockchain Technology as a Tool to Enhance Information Security Elements in the Government Organizations Sector: An Exploratory Study in the Nineveh Governorate Traffic Directorate

Saif Khalid Zakaria

Department of Management Information Systems, College of Administration and Economics, University of Mosul, Mosul, Iraq

ABSTRACT

Purpose: The objective of this study is oriented to investigate what are the determinant features of Blockchain Technology (BCT) that contribute in boosting ISE factors in governmental institutions. The research work is grounded on referring to the most popular features of Blockchain (BC) in enhancing the core and supportive (ISE).

Research Design/ Methods and approach: The data for this research was based on a cross-sectional and correlational survey (95 responses were finally analyzed). The collected data were first analyzed using SPSS v.26 and then through variance based structural equation modeling (SEM; Smart PLS v.4) for assessing validity and reliability of measures, and the study hypotheses.

Findings: The findings endorsed the conceptual model. The SEM results also demonstrate that all the proposed paths contribute to support such a model as indicated by variance-based SEM. More specifically, study results show Transparency (TR), Decentralization (DE) and Non-tamper ability (NT) are the information security enhancers with high level of impact on Core and Supportive level of (ISE).

Practical implications: This paper provides insight into the issues in information security (IS), offer a potential holistic more effective solution through provision for handling (BCT) and (BC) problems. The study suggests a gradual adoption of blockchain technology in governmental organizations as it has proven effective to improve information security because of its features of transparency, decentralization and non-tamper ability, providing that adoption occurs within an integrated regulatory, technical and training framework ensuring greater efficiency in data protection, integrity and confidentiality within the government work environment.

Originality/value: The significance of this paper lies in the limited body of prior research examining this topic that investigate the relationships between (BC) and (ISE). Moreover, no previous studies have presented or developed a theoretical framework that includes the process of identifying the most influential Blockchain features on information security, especially in

Received 29 January 2026; accepted 28 March 2026.
Available online 31 March 2026

E-mail address: Saif_khalid@uomosul.edu.iq (S. K. Zakaria).

https://doi.org/xx.xxxxx/2572-5386.1567

the context of Iraq. Therefore, this study offers an original contribution through its proposed approach.

Keywords: Blockchain technology, Blockchain features, Information security, Core elements, Supportive elements, PLS-SEM

1. Introduction

The protection of information assets has become a topic of widespread interest worldwide. Under the umbrella of data security, various concepts emerge including information security (Taherdoost, 2022). (IS) is an administrative responsibility that falls on the entire organization, not just a specific department. All departments and divisions of the organization must cooperate to ensure (IS) by following a specific strategy that aligns with its goals and plans (Caballero, 2013). Preventing the loss, damage, destruction, or unauthorized access to information processed by organizations is an ongoing challenge both internally and externally and It often leads to security breaches in the different ways (Dighriri et al., 2025; Veiga & Martins, 2015).

On the other hand, (BC) is rapidly evolving and providing multiple supports for efficient data processing. It improves data sharing efficiency, highlights the value of data, and achieves effective protection and deep utilization of computer data. It also enhances the traceability of previous data (Zeng et al., 2020).

By employing this technology, Symmetric, and asymmetric encryption algorithms among others, provide multiple guarantees for computer data security, improving the effectiveness of data and (IS) protection (Li & Li, 2023; Sr et al., 2025). also, organizations can enhance their ability to address existing challenges in data traceability, sharing, and security (Li & Gong, 2022). It has become necessary for researchers, decision-makers, and practitioners to understand the characteristics that influence the acceptance of the use of (BCT) in enhancing information security in government organizations (Roopnarain & Mwapwele, 2025). as this is considered a crucial step in developing a secure and effective system based on (BCT).

This study aims to answer the following questions:

Q1. To what extent does the studied organization perceive (BCT) as a means to improve its information security?
Q2. Which specific characteristics of (BCT) hold the greatest potential to strengthen (ISE) within government organizations?
Q3. Is there a significant impact relationship between the characteristics of (BCT) in enhancing the basic and supporting elements of (IS)?

This paper adds to the (IS) literature on engaging with (BCT) as an emerging area of study and furthers understanding of its relevance for this important domain. There are multiple unique aspects of this paper. First, the researcher believes that this is the first attempt to include (BCT) potentials with main and supporting(ISE) characteristics aimed at identifying the most important characteristics affecting(IS) in systems of government organizations, particularly within Iraqi scope. Secondly, the majority of studies relied solely on descriptive research methods to examine the importance of (BCT) in the domain of (IS). As a result, we tried to create a theoretical framework and test it with appropriate statistical analysis based on two programs; Smart PLS v.4 and SPSS v.26. This questionnaire obtained 95 responses (convenience samples). The distributed questionnaire was done electronically to cover study *sample* which originally represented employees in the Nineveh Governorate Traffic

Directorate/Mosul City. This field of study was chosen because the researched organization deals with a large amount of information that is exchanged through its information system on the Internet. In addition, the surveyed organization constantly seeks to develop its work by using advanced technologies to improve the services provided.

This work is divided into six sections: Introduction, Literature Review, Hypothesis Development, Methodology, Structural Model Testing. Discussion, implications, limitations, recommendation and Contributions are covered in the final Section.

2. Theoretical background and previous studies

2.1. Blockchain technology-driven information security

Several studies highlight the potential of (BC) to enhance the security and reliability of data and information for web applications. Aliya et al. (2023) explore how Blockchain can improve data security through encryption, robust network security, and reliable information transmission. They emphasize the importance of risk management and comprehensive security strategies for Blockchain solutions. Where (Li & Li, 2023) resolved data protection in the era of the network. They focus on how (BC) characteristics like diminishing data tampering threat, swift data dissemination and distributed data processing contribute to improved security for the end-to-end solution. Regarding (Cao, 2023), he suggests a new manner of managing (IS) in digital archives through means of (BCT). Such an approach solves problems like information deviation, unavailability and confidentiality (Sabiri et al., 2025). Risks are identified and the benefits of Blockchain for information security in digital archives are considered. It also sets regulatory rules for safe storage management in a digital archive that uses (BCT).

Contrastingly, some researchers mention Beyond-Web Applications (Blockchain Applications in Other Sectors) Suma (2019) studies Blockchain as a remedy to enhance privacy and security in government and private areas. The paper introduces a new way to employ Blockchain that can support creating/validating Smart Contracts in preparation for exchange of sensitive information between organizations while minimizing, preventing inappropriate and fraudulent use. This proposed chain model makes use of digital signature and Blockchain technology for better protecting the security amount of data communication (Suma, 2019). While (Zeng et al., 2020) discusses information security issues in various parts of energy networks and how corresponding technical characteristics of Blockchain can be used to tackle them.

Rizky et al. (2021) investigate the application of (BCT) in securing information systems in education. This research demonstrates the capabilities of Blockchain in maintaining data integrity, and enabling peer to peer information exchange with no intermediary. Although there has still no large-scale real-world applications, several studies are currently investigating the usage of Blockchain-based fingerprint hashing to secure education information systems (Subburaj et al., 2025).

2.2. Benefits of previous studies

- Past studies enable us to gain some insight into (BCT) contribution in enhancing (IS) in organizations and the factors that impact it.
- The researchers after reviewing the studies they pointed out that most of the studies were concentrated on how to use descriptive research methods to mention the importance of (BC) in the (IS) discipline. Thus, our study aims to build a hypothetical model and examine it with relevant statistical methods. This provided an insight towards the research gap.

- Reviewing the studies mentioned above and other relevant studies helped shape the research proposals and build a preliminary picture of the future direction in this field.
- The six studies summarized above conclude that (BC) can be a valuable tool for improving (IS). It offers significant benefits in various domains by enhancing data security and reliability, eliminating the need for a trusted third party, achieving decentralized value processing of information's essence in a decentralized and secure manner, and ensuring that data and information cannot be easily tampered with, lost, or destroyed.

3. Conceptual model and hypotheses development

3.1. Conceptual framework

The conceptual framework of the present study was developed to examine the role of (BCT) as a Tool to Enhance (ISE) in the Government Organizations Sector (Nineveh Governorate Traffic Directorate), In our proposed model, three critical components within (BCT) are identified that affect the core and supportive (ISE), which will be explained as follows:

3.1.1. Blockchain from an information security perspective

(BCT) is a revolutionary innovation in the field of internet security (Muhammad et al., 2022). It is recognized as one of the latest technologies in the field of security, traceability, and transparency for managing any digital transactions (Ahmed, 2020). It can also be defined as a distributed ledger system that uses algorithms to manage the information content of linked and chained data blocks, supported by encryption techniques Drescher, 2017b to ensure data integrity and preservation (Aliya et al., 2023). It can also be viewed as an encrypted database (Davidson-Shivers & Rand, 2022) of an ever growing list of transaction records organized into a chain of blocks (Zhang, Xue, & Liu, 2019)), the hashing encryption (Monev, 2020). Thus, Blockchain is a distributed database which forms a chain of blocks connected to one another by means of private encryption and timestamp. Each block contains the hash of the previous block, thus forming a chain of linked blocks that are difficult to change. It is based on a peer-to-peer network that eliminates the need for a mediator (third party), which increases user confidence in this technology (Al-Shammari, 2023).

Shrier et al. (2016) pointed out that the importance of (BCT) in enhancing (IS) lies in the fact that traditional data security models rely on creating protection methods by adding multiple authentication factors to access data and using stronger encryption. However, Al-Shammari (2023)explained that these models generally weaken once you enter the system, as it becomes possible to access the data. with (BCT), the data silos are dispersed, which reduces the set of possible breaches that data can be exposed (Berdik et al., 2021). This provides a more secure way to store and access data, which enhances the ability of data managers to protect critical information for their organizations. Shrier et al. (2016) also pointed out that the basis of all (BCT) applications is the importance of securing data and information by adopting distributed computing and zero-knowledge protocols. This essentially allows data to be used while ensuring its privacy within the concept of a trusted network. McEvily et al. (2021) referred to this as the general positive expectations about the motivations, intentions, and behaviors between actors who are not directly connected, but who participate in a limited social structure of a set of network computers and legal rules that define and govern everything related to data expectations (Manu et al., 2020).

(BCT) consists of a variety of components that include, according to the opinions of the authors (Aggarwal & Kumar, 2021; Al-Shammari, 2023; Patel et al., 2020; Pohl et al.,

Table 1. Key properties of blockchain.

source	Decentralization	Non-tamper ability	Verification and tracking	Trust	Collective maintenance	Database reliability	Transparency	Security	Anonymity	Programmability and intelligent implementation
(Dbesan et al., 2023)	✓	✓	✓					✓		✓
(Al-Shammari, 2023)				✓			✓	✓		
(Patricio & Ferreira, 2021)							✓	✓		✓
(Shen et al., 2020)	✓	✓	✓							
(Xinyi et al., 2018)	✓	✓	✓	✓	✓	✓	✓		✓	✓
(Bartling & Fecher, 2018)	✓	✓					✓			
(Zheng et al., 2017)	✓	✓					✓			
Total	**5**	**5**	**3**	**2**	**1**	**1**	**5**	**3**	**1**	**3**
percentage	**62.5**	**62.5**	**37.5**	**25**	**12.5**	**12.5**	**62.5**	**37.5**	**12.5**	**37.5**

Source: table by author.

2020) from (Blocks, Transactions, Timestamps, Consensus Algorithms, Nodes, Mining and Smart Contracts), These components work across various devices in a distributed manner that is completely different from the concept of centralized and decentralized networks.

Such properties of (BCT) offer companies an alternative to change the way of conduct administrative or business processes. A large-scale business process management (BPM) vendor today, indeed struggles with the conflicting feature require- mentsand trade-offs of scalability, security, openness trusted and cost when accommodating new technology such as Blockchain (Viriyasitavat & Hoonsopon, 2019).

n the latest years, an array of blockchain platforms was proposed and implemented based on security application scenarios. This allows to conduct secure transactions among an untrusted set of players (Conoscenti et al., 2016). The technology has many good behaviors and characteristics, which are inherently proper for preserving sharing data integrity (Shen et al., 2020). The main properties of (BCT) are summarized in Table 1

Considering Table 1, we observe that these core properties (DE, NT and TR) are those which have the highest consensus according to the sources listed in it. Since they are fundamental to the field and easily described, these properties will be used as a basis for our present study:

1. **Transparency (TR):** Denotes the means of information disclosure, honest and fair access to, and checking the transactions carried out over the (BC) network. It will contribute to the transparency of these transactions and facilitate access to them (Al-Shammari, 2023).
2. **Decentralization (DE):** It is the most salient and essential property of BC systems. In a distributed scheme, the tasks of recording, storing, sending/receiving, verifying and retaining data are conducted throughout the network by nodes via asymmetric encryption. This avoids the need for a central authority, which could tweak it's data as it pleases. The distributed node is relatively independent; the problem and the exception of a certain node do not affect data systems. The reliability and robustness of (BC) systems are largely improved with the help of this model (Xinyi et al., 2018).
3. **Non-tamper ability (NT)**: It is an important feature of (BCT) which doesn't let alter the data that is stored in it by deploying a distributed checking process, where all nodes participating in the network have to okay any change. It builds an interdependent web of digital evidence that preserves the integrity of the content. There is no

sense of making a partial change and we can't control nor modify (5%) nodes in the network at with the same time. This is almost impossible with the distributed and wide network propagation network (Li & Gong, 2022).

3.1.2. Information security (concept, importance, and elements)

In the digital age, information, its applications, and various technological tools have become the main drivers of competition. In contrast, organizations face various threats and risks related to their information security (Shaheen, 2020).

The origin of information systems security dates back to the late 1970s when it was referred to as "communications security" (Ali, 2009). With the growth of personal computers in the 1980s, a new era began in the field of security, called computer security. It was defined as "the standards and procedures that ensure the confidentiality, integrity, and availability of information system components, including hardware, software, and processed, stored, and transferred information" (Raouf & Raouf, 2022).

In the 1990s, the concepts of communication security and computer security were merged to form what is now known as "information systems security" (Raouf & Raouf, 2022). Aldabbagh (2022) defines it as "the state of affairs that relates to measures and procedures to protect information stored in the database system from unauthorized use, whether intentional or unintentional, by countering attempts to transfer, modify, or destroy data protection software" (Al-Salmi, 2000).

From a technical perspective, O'brien (1990) states that (IS) refers to the necessary means, tools, and procedures that must be provided to ensure information protection against internal and external threats.

Based on the above, the researchers agree with the Caballero (2013) definition of (IS) as the protection of an organization's assets from disruption of business operations, falsification of sensitive data, or disclosure of confidential information. This is achieved by maintaining the confidentiality, integrity, and availability of the organization's assets, operations, and information.

In light of the above, we find that the importance of (IS) has been formed and the need for it has increased with the continuous information explosion that requires multi-faceted protection of the organization's information (Al-Yahyawi, 2010). AL-Abid (2020)explained that the importance of (IS) lies in:

1. Providing accurate and correct information to economic sectors due to the rapid growth in the use of electronic applications.
2. The existence of applicable security procedures that cover the risks that may arise when dealing with multiple parties.
3. Building a secure electronic environment that serves the public and private sectors.
4. Protecting the information network infrastructure to ensure the correct flow of transactions.

In this context, the researchers (Al-Qahtani, 2015; Andress, 2014; Merkow & Breithaupt, 2014; Shaheen, 2020) emphasize the importance of (ISE). When implemented effectively, it creates a secure environment for electronic transactions. Conversely, neglecting any of these elements creates vulnerabilities that could be exploited compromising an organization's security.

Al-Qahtani (2015) explained that these elements are the set of requirements that must be met to protect static and transmitted information, These elements must be integrated to provide the required protection. Failure of any of these elements will affect the security of the aspect covered by that element.

The following section will detail these critical (ISEs).

Information Security Elements:.

1. **Information Availability (IA):** It ensures the continuous operation of the information system and the ability to continuously process information and provide service to information sites when needed by authorized persons. This aspect of security aims to ensure the continuous availability of information over time while providing immediate and effective service to beneficiaries (Andress, 2014).
2. **Integrity (IN):** reflects the quality of any information system through its accuracy and reliability, as well as its logical integration with its hardware and software. This aspect of security reflects the harmony of the information structure with the stored data and the proper integration of the various mechanisms that provide protection. It aims to protect information from manipulation or corruption and to ensure its continued quality and accuracy over time. In other words, it preserves the integrity and completeness of data and information during the operation of information systems (Al-Qahtani, 2015).
3. **Confidentiality of Information (IC):** Also known as, privacy. This element restricts access to data and information assets to authorized individuals and organizations. It emphasizes the importance of not disclosing information to unauthorized parties. This aspect of security is crucial for ensuring the privacy of information and protecting it from unauthorized access (Shaheen, 2020).
4. **Information Integrity (IE):** refers to ensuring the correctness of the content of information. This means verifying that the content has not been modified or tampered with. It emphasizes the importance of preventing the destruction, alteration, or manipulation of content at any stage of processing or exchange, whether during the internal handling of information or through unauthorized intervention (Andress, 2014).
5. **Non-repudiation (NR):** Assuring that the person performing a specific action related to information or its location cannot deny or refute that they were the one who performed that action. This assurance allows for the possibility of proving that the action was performed by the person concerned at the appropriate time (Merkow & Breithaupt, 2014).
6. **Authentication (AU):** Verifying the identity of a person or entity and ensuring that they are the person or entity authorized to access the information. In the case of information transfer, the identity of the sender must be verified to ensure that the message comes from its true source, and the same applies to the recipient of the message.
7. **Access Control (AC):** The methods that control user access to the resources of the information system. It also helps in determining the level of authorized access, which does not only apply to users but also restricts the access of other systems to information resources (Liu & Xu, 2018).
8. **Auditing (AD):** Monitoring and recording user operations on resources to review them and identify any irregularities or unauthorized access (Al-Qahtani, 2015).

We can observe from Table 2 that the (ISEs) that have been agreed upon with high percentages are (IA = 100%), (IN and IC = 87.5%), and (IE = 62.5%), these three elements represent the core elements. The other elements (NR, AU, AC, and AD) are considered supporting elements that can enhance information security in digital transactions.

3.1.3. Blockchain technology and information security in government organizations

Government organizations face increasing challenges in the field of (IS). The amount of data and information that these organizations deal with is increasing due to the digital

Table 2. Information security elements.

source	AU	AC	IC	IN	IE	NR	IA	AD
(Al-Qahtani, 2015)	√	√	√	√	√	√	√	√
(Kaushal & Khan, 2018)	√	√	√	√	√	√	√	√
(Singh et al., 2014)			√	√	√		√	
(Merkow & Breithaupt, 2014)			√	√	√	√	√	
(Shaheen, 2020)			√		√		√	
(Bhatnagar, 2007)			√	√			√	
(Al-Fayhan & Gharib, 2015)			√	√			√	
(Blackley et al., 2004)				√			√	
Total	**2**	**2**	**7**	**7**	**5**	**3**	**8**	**2**
percentage	**25%**	**25%**	**87.5%**	**87.5%**	**62.5%**	**37.5%**	**100%**	**25%**

Source: Table by author.

growth and development witnessed by government organizations. In contrast, the risks that this information is exposed to from cyberattacks and others are increasing.

(BC) is a promising technology that can help strengthen (ISE) in the government organization sector. (BC) has many characteristics that make it suitable for (IS) applications, the most important of which is decentralization. (BCT) built on a peer-to-peer network; which means that there is no third party that may control the data. This makes it more secure than centralized systems.

(BC) also uses consensus protocols, to ensure that data cannot be tampered with or modified. This makes it ideal for recording financial transactions or any other type of data that must be reliable and secure. This is known as non-tamperability.

All participants in a Blockchain network can access the data stored on it, which makes it transparent.

Based on the proposed model illustrated in Fig. 1 and the rationale discussed above, the following hypotheses are proposed:

H1: There is a significant difference in the relative importance of the research variables (BC and IS) according to the opinions of the sample in the studied organization.
H2: (TR) morally affects the strengthening of (IA) as an essential element of (IS).
H3: (TR) morally affects the strengthening of (IE) as an essential element of (IS).
H4: (TR) morally affects (AU) as a supporting element of (IS).
H5: (TR) morally affects (AC) as a supporting element of (IS).
H6: (DE) morally affects the strengthening of (IA) as an essential element of (IS).
H7: (DE) morally affects the strengthening of (IN) as an essential element of (IS).
H8: (DE) morally affects the strengthening of (IC) as an essential element of (IS).
H9: (DE) morally affects the strengthening of (AD) as a supporting element of (IS).
H10: (NT) morally affects the strengthening of (IE) as an essential element of (IS).
H11: (NT) morally affects (NR) of information as a supporting element of (IS).
H12: (NT) morally affects (AC) as a supporting element of (IS).

4. Methodology

4.1. Survey instrument development

To test the proposed model, a survey has been constructed in order to measure employee perceptions from the Traffic Directorate of Nineveh Governorate. The purpose of this survey is to uncover the critical dimensions of (BCT) that influences (IS) strengthening in public organizations. The research has two variables, one is independent variable, that (BCT), and the other is dependent variable that (ISE). Three characteristics were included

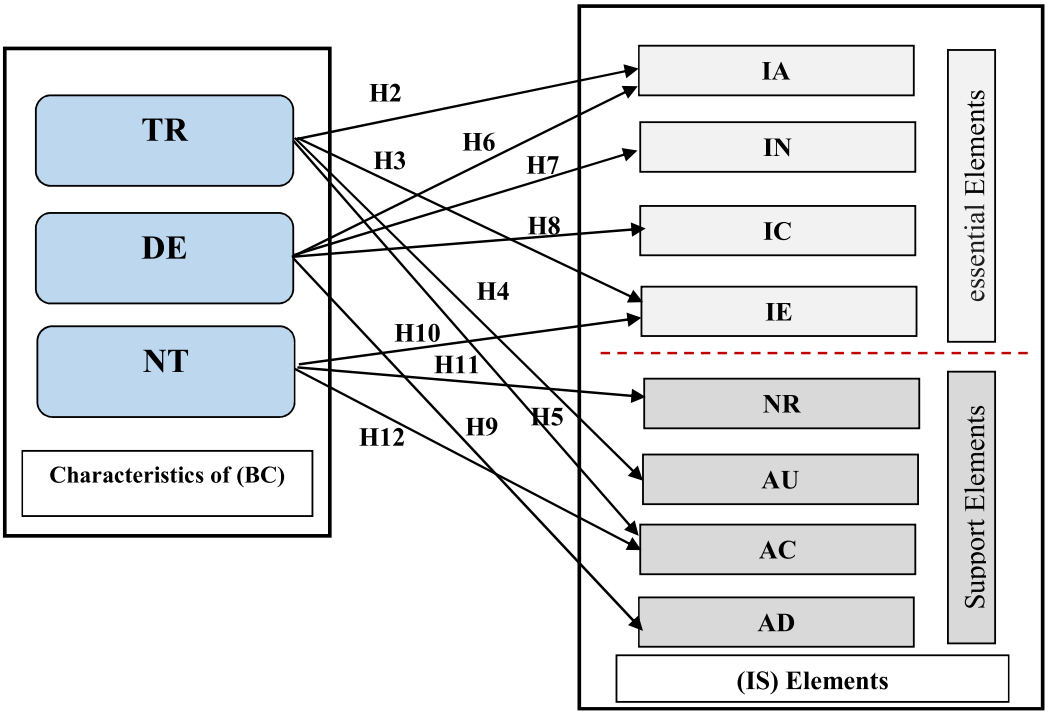

Fig. 1. Proposed conceptual model.

in the (BCT) variable, with 4 indicators for each characteristic. The dependent variable, (IS), consisted of eight dimensions each with three indicators.

The questionnaire adopted in this study is structured into three sections. Section A: Demographic profile of the respondents. In addition, the independent and dependent variables are listed in Sections B and C respectively by (32) measurement indicators that were included for measuring the study's constructs. These indexes were modified, revised, and verified by expert teachers according to the aims of this study. Agreement with the statements was ranked using a five-point Likert scale.

This research design was cross-sectional; it explored the areas of study and within the period. Data Collection The electronic survey was initiated for distribution starting October 2023. Respondents were given a deadline until February 2024. After performing checks and audits, a total of 95 valid responses was retained for final analysis. The statistical analysis was conducted with the aid of two software packages (Smart PLS v.4 and SPSS v.26).

4.2. Descriptive statistical analysis results of (BC) characteristics and (ISE) variables

Table 3, shows the results of the descriptive statistical analysis of the dimensions of (BC) and basic and supporting (ISE) for the research sample. In terms of the overall mean (median parameters for their responses), (the level of dispersion of those responses around the hypothetical mean of the measurement tool (3)), and the analysis of the relative importance of the variables in terms of their percentage weight.

Based on the above, the first main hypothesis (H1), which states, "There is a significant difference in the relative importance of the research variables (BC and IS) according to the opinions of the sample in the studied organization" **can accepted.**

Table 3. Descriptive statistical analysis of the dimensions.

The variable	Mean	SD	Weight %
BC Characteristics			
TR	3.52	1.059	10.875
DE	3.457	1.18	12.125
NT	3.458	1.243	12.75
Basic elements of information security			
IA	3.47	1.184	12.167
IN	3.497	1.022	10.467
IC	3.633	1.051	10.767
IE	3.607	0.906	9.3
Auxiliary elements of information security			
NR	3.537	0.969	9.9
AU	3.587	0.926	9.467
AC	3.54	0.891	9.167
AD	3.613	0.898	9.2

Source: table by author.

Table 4. Convergent validity of the research model.

Variables		Composite Reliability (CR)	Average Variance Extracted (AVE)	Cronbach's Alpha (α)	Rho De Joreskog
Comparison standard		> 0.70	> 0.50	> 0.70	> 0.70
Blockchain characteristics					
1	(TR)	0.881	0.651	0.821	0.829
2	(DE)	0.907	0.709	0.861	0.865
3	(NT)	0.926	0.757	0.893	0.896
Information Security Elements					
4	(IA)	0.908	0.767	0.848	0.849
5	(IN)	0.875	0.700	0.786	0.786
6	(IC)	0.902	0.754	0.838	0.852
7	(IE)	0.869	0.690	0.776	0.804
8	(NR)	0.876	0.703	0.789	0.801
9	(AU)	0.876	0.702	0.789	0.806
10	(AC)	0.837	0.632	0.707	0.715
11	(AD)	0.883	0.716	0.803	0.829

Source: table by author.

4.3. Assessment of measurement model

Any research foundation requires initially testing the research measurement model, which is represented by the validity and reliability tests of the research questions. This is to ensure, from the beginning, the ability of the data to measure what it was built for (validity), as well as the ability to measure under different circumstances (reliability). This is done by relying on the measurement of convergent validity and discriminant validity.

Convergent validity analysis requires the following three methods to reveal the validity and reliability of the measurement model in interpreting its intended meaning. These methods are (Composite Reliability (CR), Average Variance Extracted (AVE), and Cronbach's Alpha (α) values). After conducting the analysis using the Smart PLS program, the results appeared as shown in Table 4.

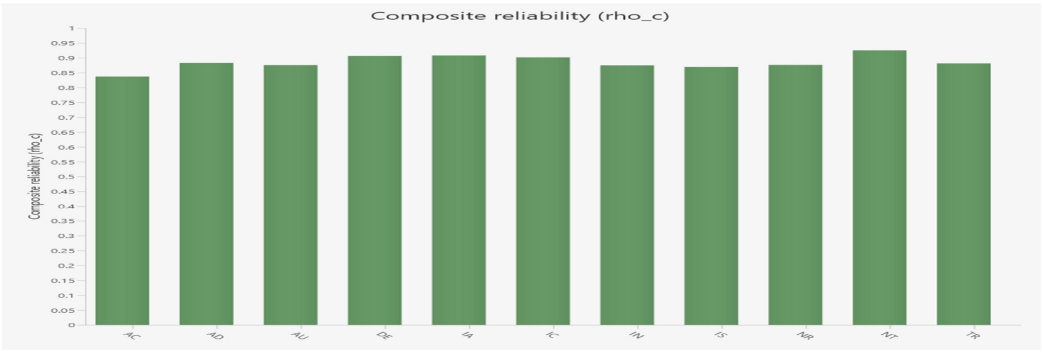

Fig. 2. Composite reliability diagram.
Source: by author.

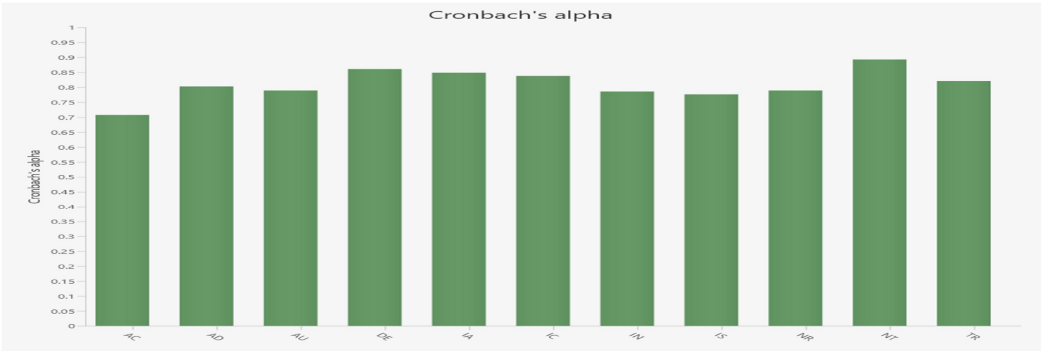

Fig. 3. Cronbach's alpha diagram.
Source: Figure by author.

By following the results of the table above, it is clear that the model obtained high convergent validity, as the composite reliability (CR) values for all variables exceeded (0.70). This was confirmed by Hair et al. (2017) when they indicated that the (CR) coefficient ranges between (0 and 1), and is considered acceptable when its value is equal to (0.7) or higher. The average variance extracted (AVE) also exceeded the acceptable value (0.50). As for the Cronbach's alpha coefficient shown in the table, the results showed that there is high reliability for the items of the study scale, as their results ranged between (0.707-0.893). In comparison, Low et al. (2017) stated that the Cronbach's alpha coefficient value should be greater than (0.7). In light of the previous results, we find that the values of the technical characteristics of (BC) and the values of the basic and supporting (ISE) are characterized by convergent validity. which indicates that the defined concepts, measure a single concept and are statistically acceptable without deleting any of the study items related to these variables, as shown in (Figs. 2 and 3) as well.

Discriminant validity refers to the logical separation of questions for a variable without repetition or overlap with other variables. It can be obtained through two tests. First Cross-loading test This measures whether a specific question measures the variable for which it was constructed, and not other variables (Li et al., 2020). All of the results of this test were positive.

Second Correlation between latent variables, This test can be obtained according to the Fornell & Larcker (1981) criterion as follows**:**

Outer Loading: The outer loading index refers to the external saturation of the dimension items (as shown in Table 5 and Fig. 4). It is considered significant at a saturation level

Table 5. Outer loading.

Variables/Loading					
(BC) characteristics	**(TR)**	**X1**	**X2**	**X3**	**X4**
	Loading	0.832	0.793	0.752	0.845
	(DE)	**X5**	**X6**	**X7**	**X8**
	Loading	0.879	0.729	0.858	0.893
	(NT)	**X9**	**X10**	**X11**	**X12**
	Loading	0.900	0.881	0.827	0.870
(IS) Elements	**(IA)**	**Y1**	**Y2**		**Y3**
	Loading	0.868	0.876		0.884
	(IN)	**Y4**	**Y5**		**Y6**
	Loading	0.807	0.868		0.834
	(IC)	**Y7**	**Y8**		**Y9**
	Loading	0.890	0.841		0.872
	(IE)	**Y10**	**Y11**		**Y12**
	Loading	0.783	0.815		0.890
	(NR)	**Y13**	**Y14**		**Y15**
	Loading	0.790	0.876		0.847
	(AU)	**Y16**	**Y17**		**Y18**
	Loading	0.852	0.792		0.867
	(AC)	**Y19**	**Y20**		**Y21**
	Loading	0.833	0.821		0.727
	(AD)	**Y22**	**Y23**		**Y24**
	Loading	0.864	0.890		0.781

Source: Table by author.

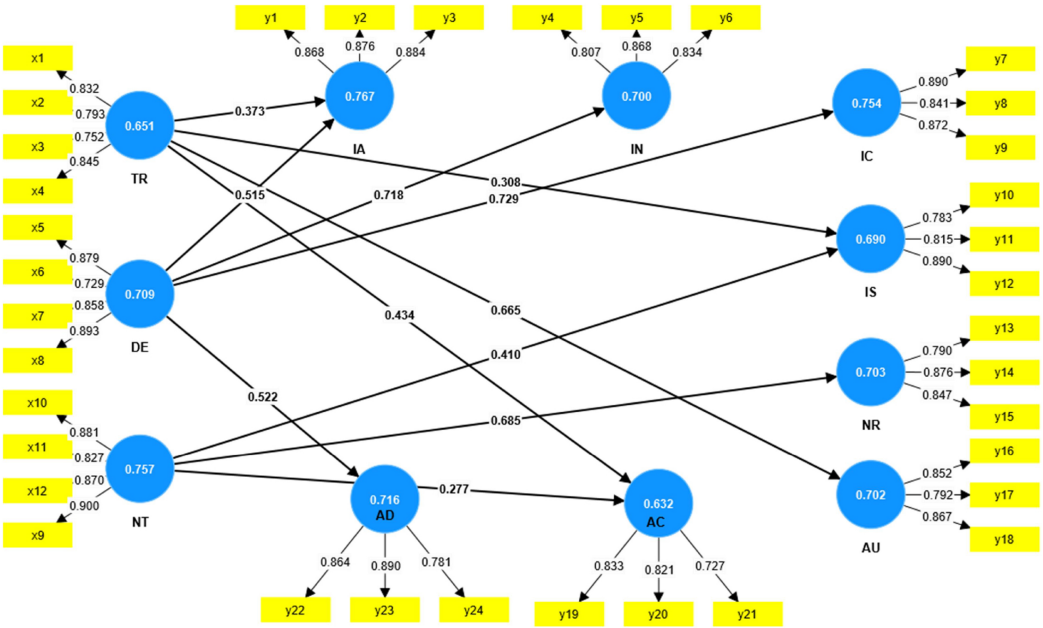

Fig. 4. Outer loading values for the research variables.
Source: Figure by author.

of (0.70). If the saturation is between (0.40 and 0.70), we need to examine the impact of these items on the possibility of raising the composite reliability value. If deleting these items does not affect the increase in the composite reliability value, then they are retained. However, if the saturation is less than 0.40, the item is deleted. Therefore, in this study, we relied on the items with a saturation level of 0.70 or higher.

Table 6. Correlation matrix between latent variables.

	AC	AD	AU	DE	IA	IC	IN	IE	NR	NT	TR
AC	**1.000**										
AD	0.779	**1.000**									
AU	0.811	0.710	**1.000**								
DE	0.578	0.522	0.551	**1.000**							
IA	0.529	0.581	0.630	0.745	**1.000**						
IC	0.573	0.543	0.619	0.729	0.811	**1.000**					
IN	0.666	0.738	0.571	0.718	0.765	0.754	**1.000**				
IE	0.741	0.681	0.661	0.607	0.640	0.661	0.718	**1.000**			
NR	0.779	0.648	0.729	0.608	0.595	0.577	0.644	0.729	**1.000**		
NT	0.574	0.563	0.603	0.732	0.840	0.658	0.712	0.621	0.685	**1.000**	
TR	0.624	0.622	0.665	0.618	0.691	0.602	0.574	0.589	0.544	0.686	**1.000**

Source: Prepared by author.

Consequently, all of the external saturations of the scale items are greater than the lower limit set by Hair et al. (2014), as they all exceeded the significant saturation values as shown in Table 5. Therefore, the data for the study variables are suitable for statistical analysis.

Correlation Matrix: This test refers to the dimensions of correlated data characteristics. This process is achieved when the loading of items on their scales is greater than their loading on other scales (Li et al., 2020). This means that any variable must have a higher correlation with itself than with any other variable to be considered stable. For example, decentralization (DE) had a correlation with itself of 100%, which is higher than all the correlation values with other variables within the same column or row. In addition, other variables were highly correlated with themselves, as shown in Table 6. Therefore, this is an important indicator for moving on to the hypothesis testing.

5. Structural model evaluation

Assessing the structural model is essential for validating the study's proposed relationships. This step determines whether the collected data supports the hypotheses derived from the conceptual model (Al-Shammari, 2023). In PLS-SEM the structural model can be evaluated using the coefficient of determination (R^2), the effect size (F^2), the beta coefficient (β), the T-value and the P-value (Mohamed et al., 2018), as follows:

Table 7. Test structural model of study (Hypothesis testing).

No. H	Hypothesis	Path coefficients	T Statistics	F^2	P Values	Decision
H2	TR -> IA	0.373	3.116	0.122	0.002	Accepted
H3	TR -> IE	0.308	2.404	0.061	0.016	Accepted
H4	TR -> AU	0.665	11.909	0.761	0.000	Accepted
H5	TR -> AC	0.434	3.383	0.083	0.001	Accepted
H6	DE -> IA	0.515	4.186	0.354	0.000	Accepted
H7	DE -> IN	0.718	13.937	0.661	0.000	Accepted
H8	DE -> IC	0.729	14.798	0.631	0.000	Accepted
H9	DE -> AD	0.522	6.309	0.057	0.000	Accepted
H10	NT -> IE	0.410	3.111	0.272	0.002	Accepted
H11	NT -> NR	0.685	11.342	0.549	0.000	Accepted
H12	NT -> AC	0.277	2.085	0.024	0.037	Accepted

Source: by author.

Table 7 and Fig. 5 shows positive direct effect which is significant between Transparency (TR) and Information Availability (IA) with ($\beta = 0.373$; T = 3.166; P = 0.002) These results provide support for *H2*. The impact relationship between (TR) and Information Integrity

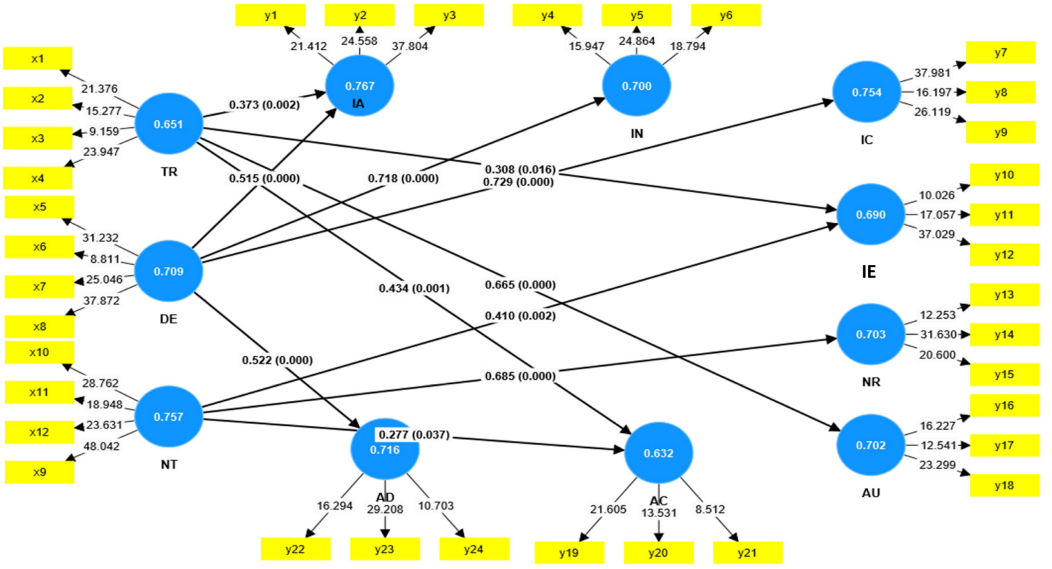

Fig. 5. Study's structural model.
Source: figure by author.

(IE) is positive, direct and only get significant value from data sample(n = 147) with values of (β = 0.308; T = 2.404; P = 0.016) These results support the *H3*. There was a significant positive direct and impact of (TR) on Authentication (AU)(β = 0.665; T = 11.909; P = 0.000). These results are supportive of the *H4*. The effect relationship between (TR) and Access Control (AC) is significant Positive direct (β = 0.434; T = 3.383; P = 0.001). These data support the *H5*.

The outcome revealed positive direct and significant effect of Decentralization (DE) on Information Availability (IA), with path value (β = 0.515; T = 4.186; P = 0.000), respectively. Such findings reinforce the *H6* case. Decentralization (DE) and Integrity (IN) have positive, direct and significant effect Relationship (β = 0.718; T = 13.937; P = 0.000), These results support the *H7*. A positive, direct and important interface was found between (DE) and (IC) (β = 0.729; T = 14.798; P = 0.000). These findings support *H8*. The impact relationship between Decentralization (DE) and Auditing (AD) is negative, direct and significant (β = -0.522; T = 6.309; P = 0.000). These data support the H9.

The results further showed a positive direct and significant impact relationship between Non-tamper ability (NT) and Information Integrity (IE) (β = 0.410; T = 3.111; P = 0.002). These findings support the H10. The effect relationship between Non-tamper ability (NT) and Non-repudiation (NR) of information is positive, direct and significant (β = 0.685; T = 11.342; P = 0.000). These results support the H11. Finally, the results showed a positive, direct, and statistically significant effect of non-tamper ability (NT) on access control (AC) (β = 0.227, T = 2.085, p = 0.037). Therefore, H12 was supported.

The results of the coefficient of determination (R^2) shown in Table 8 indicate that the independent variables explain an acceptable to high proportion of the variance in the dependent variables, which reflects the model's adequacy and predictive power. According to Hair et al. (2017), values exceeding 0.25 are considered indicative of an acceptable explanatory strength in social and administrative studies. With regard to the effect size (f^2), the findings revealed that some relationships exhibit very strong effects (such as the relationship between DE and IC/IN, or TR and AU), while others showed medium and weak effects. This highlights the varying relative contributions of the variables within the

Table 8. Coefficient of determination (R^2) and effect size (f^2) results.

Endogenous Variables	R^2	R^2 Adjusted	f^2 (Effect Size from Exogenous) Variables)	Cohen's Classification
AC	0.430	0.417	TR → AC = 0.175	Medium
AD	0.273	0.265	DE → AD = 0.375	Large
AU	0.442	0.436	TR → AU = 0.793	Large
IA	0.642	0.634	DE → IA = 0.456, TR → IA = 0.240	Large, Medium
IC	0.531	0.526	DE → IC = 1.132	Large
IN	0.516	0.510	DE → IN = 1.065	Large
IE	0.437	0.424	TR → IE = 0.089, NT → IE = 0.158	Small, Medium
NR	0.469	0.463	NT → NR = 0.883	Large

model, which is consistent with Cohen's (2013) classification of f^2 values as weak (0.02), medium (0.15), and strong (0.35) (Cohen, 2013). Overall, this provides a more precise picture of the model's dynamics.

6. Discussion

The current study sought to clarify the role that the characteristics of blockchain technology may play in enhancing the elements of information security within governmental organizations, based on the fact that the governmental environment suffers, to varying degrees, from challenges related to data integrity, data protection, and reliability in administrative work. Through the analysis of the results of the statistical model, it was found that the study achieved a set of indicators demonstrating the quality of measurement and the strength of the structural relationships among the variables. The measurement results confirmed that the research instruments possess acceptable statistical validity and reliability, as the composite reliability (CR) values for all variables exceeded the threshold of (0.70), and the average variance extracted (AVE) values exceeded the acceptable value of (0.50), which is consistent with the criteria proposed by Hair et al. (2017) regarding the adequacy of the structural model. In addition, Cronbach's alpha values indicated a high level of reliability for the scales, ranging between (0.707–0.893), in line with what was reported by Low, Gefen et al. (2000) indicating that the model was able to measure the variables accurately without the need to delete any items.

Furthermore, with regard to testing the structural model, the values of correlation coefficients and path coefficients revealed the existence of significant relationships between the characteristics of blockchain technology and the elements of information security. The bootstrapping test results showed direct and statistically significant effects at the level of ($P < 0.05$), providing empirical support for the research hypotheses. These included the effect of transparency on information availability and integrity, the effect of decentralization on information integrity and confidentiality, and the effect of tamper resistance on non-repudiation and access control. Based on the above, these results are consistent with the theoretical structure of blockchain technology, as it relies on a distributed ledger, decentralization, and immutability of content, all of which are characteristics theoretically associated with data security, as explained by Drescher (2017a). They also support findings in the literature regarding the contribution of transparency to enhancing institutional trust (Madanchian & Taherdoost, 2025) and improving data traceability (Underwood, 2016), making blockchain technology suitable for sensitive applications such as those in the governmental sector.

In addition, the values of the coefficient of determination (R^2) demonstrated a considerable explanatory power of the model, as the adjusted R square values for some variables fell

within the medium to high range, such as (IA) with a value of (0.634), (IC) with a value of (0.526), and (AU) with a value of (0.436), in accordance with the recommendations of Hair et al. (2017). This indicates the ability of the independent variables to explain a significant proportion of the variance in information security elements, thereby enhancing the validity and predictive power of the model. The descriptive results of the survey also suggested that participants (respondents) possessed a moderate to high awareness about characteristics of blockchains, with an overall mean score for blockchain characteristics being (3.478), as its standard deviation was found to be (1.161), and this for information security dimensions was (3.561). This further implies a degree of putting this technology to work in the type of government we are after, even when it involved protecting and preventing data from being altered.

In light of the above, it is possible to say that findings not only confirm the validity of the model proposed, but also open up avenues for a more extended view on blockchain applications in government area, particularly if we consider those countries that are still constructing their digital environment. Institutional trust, security weaknesses, and challenges with central systems can be addressed under the rubric of provision of institutional blockchain features as a strategic point of entry. This is the contribution of the study in terms of knowledge by exploring information security as part explaining information security in government sector from the perspective on emerging technologies.

6.1. Limitation

This study has several limitations, the first of which is its cross-sectional nature that could affect the associations and restrict inferences over temporal changes. It is consistent to suggest that longitudinal investigation needs to be considered in future studies, as it would help to monitor the changes in the effect of these variables on BCT across time thus furthering our knowledge regarding process dynamics.

6.2. Recommendation

Considering the results of current study that validated the effectiveness of blockchain technology elements, especially (transparency, decentralization and non-tamper ability) in enhancing information security components in governmental organizations, the following recommendations are offered to help the effective and organized implementation of this technology in public sector.

- Based on this, the researcher recommended that governmental organizations should consider implementing blockchain technology in stages and also at least, but not limited to at systems with sensitive data and key transactions requiring high levels of security, reliability and accountability.
- This study also finds the necessity of well consideration or a good design (E-Document) when upgrading existing design by emphasizing on the features attributes such as transparency, decentralization and non-tamper ability attributes from Blockchain top down initially, as they will become nice digital systems to be sure we achieve the enhancement in information security that is anticipated from blockchain.
- We strongly advise against the implementation of any blockchain solution that does not integrate with an operational process technology stack, which will ensure such disruption is executed in a safe and efficient manner through digitization.
- Introduction of a comprehensive regulatory and organizational framework for its implementation in blockchain even covering aspects like access control (role-based

vs rule-based), user authorization, monitoring as well as auditing policies which are somewhat closer to data governance.
- The researcher further suggests that government institutions have specialized training programmed for employees to enhance his or her technical understanding of victories and its functionality as well the ability to implement block chain enterprise systems to accordance information security specifications.
- Finally, the study indicates that pilot blockchain will be attainable in particular government authorities where data exchange, documentation and verification are high frequency to gradually realize the effective and expansive application for this CIT into the future.

7. Contributions

This research contributes to the current knowledge base in several ways:

- Addressing a knowledge gap: The research bridges a gap in understanding the impact of blockchain technology on information security in public sector institutions.
- Providing practical recommendations: The research offers practical recommendations to enhance information security in public sector institutions through the adoption of (BCT).
- Stimulating further research: The findings open avenues for further studies on the applications of blockchain technology in various aspects of public sector management.

Ethical approval

Due to the absence of a formal Research Ethics Committee at the University of Mosul at the time of the study, the research was conducted in strict adherence to international ethical standards. As this is a survey-based study, informed consent was obtained from all participants. Participation was entirely voluntary, and respondents were clearly informed of their right to withdraw from the study at any time without any obligation.

Conflict of interest

The author declares no conflict of interest.

Author contribution

The author confirms sole responsibility for the following: study conception and design, data collection, analysis and interpretation of results, and manuscript preparation. The author has reviewed and approved the final version of the manuscript and takes full responsibility for the accuracy of the information provided.

Data availability

The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

References

Aggarwal, S., & Kumar, N. (2021). Chapter Ten - Core components of blockchain: Introduction to blockchain. In S. Aggarwal, N. Kumar, & P. Raj (Eds.), *Advances in Computers* (Vol. 121, pp. 193–209). Elsevier. https://doi.org/10.1016/bs.adcom.2020.08.010.

Ahmed, M. (2020). *Blockchain in Data Analytics* (first ed.). Cambridge Scholars Publishing.

AL-Abid, S. (2020). Information security through social media The case of Facebook. *Arab Journal of Informatics and Information Security*, *1*(1), 201-218. https://doi.org/10.21608/jinfo.2020.114719.

Al-Fayhan, E. A., & Gharib, A. H. A. (2015). The Evaluation of Information Security Management System in the Iraqi Commission for Computers and Informatics according to the International Standard (ISO 27001: 2013) *journal of Economics And Administrative Sciences*, *21*(86), 1–26. https://doi.org/10.33095/jeas.v21i86.764.

Al-Qahtani, T. b. A. (2015). *Information Security* (first ed.). KACST.

Al-Salmi, A. A. R. (2000). *Information Technology* (3 ed.). Dar Al-Manahij for Distribution and Publishin.

Al-Shammari, A. H. D. (2023). *Adopting Blockchain Technology Driven Knowledge Management in Health Organizations: A Survey Study in Mosul Governmental Hospitals* Mosul]. Unpublished.

Al-Yahyawi, Y. (2010). *On Communicability: Communication at the Test of the Internet and the Globalization of Information*. Okaz Publications.

Aldabbagh, A. h. t. (2022). The impact of information security on digital education An exploratory study in some formations of the Northern Technical University (Technical Institute/Mosul and Ninevea) *Tikrit Journal of Administration and Economics Sciences 18*(59 part 1), 112-126. https://doi.org/10.25130/tjaes.18.59.1.7.

Ali, A. A. M. (2009). System of information security in business organizations with a proposed model to meet the threats of the system *Iraqi Journal for Administrative Sciences*, *6*(23), 219-237.

Aliya, B., Olga, U., Yenlik, B., & Sogukpinar, I. (2023). Ensuring Information Security of Web Resources Based on Blockchain Technologies. *International Journal of Advanced Computer Science and Applications*, *14*(6). https://doi.org/10.14569/ijacsa.2023.0140689.

Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress.

Bartling, S. n., & Fecher, B. (2018). Blockchain for science and knowledge creation. In *Gesundheit digital: Perspektiven zur Digitalisierung im Gesundheitswesen* (pp. 159-180). Springer. https://doi.org/10.1007/978-3-662-57611-3_10.

Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A Survey on Blockchain for Information Systems Management and Security. *Information Processing & Management*, *58*(1), 102397. https://doi.org/10.1016/j.ipm.2020.102397.

Bhatnagar, A. (2007). Need of Information Security In The 21st Centuary: With Special Emphasis to Computer Security.

Blackley, J. A., Peltier, T. R., & Peltier, J. (2004). *Information security fundamentals*. Auerbach Publications.

Caballero, A. (2013). Information security essentials for IT managers: Protecting mission-critical systems. In *Computer and information security handbook* (pp. 379–407). Elsevier. https://doi.org/10.1016/B978-0-12-394397-2.00021-0.

Cao, Q. (2023). Research on Information Security Protection Strategy of Digital Archives Based on Blockchain Technology. Proceedings of the 4th International Conference on Modern Education and Information Management, ICMEIM 2023, September 8â€ “10, 2023, Wuhan, China, http://www.doi.org/10.26855/acc.2023.04.005.

Cohen, J. (2013). *Statistical power analysis for the behavioral sciences*. routledge.

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), http://www.doi.org/10.1109/AICCSA.2016.7945805.

Davidson-Shivers, G., & Rand, A. (2022). Asynchronous Tools for Interaction and Collaboration. In *Handbook of Open, Distance and Digital Education* (pp. 1–18). Springer. https://doi.org/10.1007/978-981-19-0351-9_56-1.

Dbesan, A. H., Abdulmuhsin, A. A., & Alkhwaldi, A. (2023). Adopting knowledge-sharing-driven blockchain technology in healthcare: a developing countryâ€ ™s perspective. *VINE Journal of Information and Knowledge Management Systems*, *55*(ahead-of-print), 683–709. https://doi.org/10.1108/VJIKMS-01-2023-0021.

Dighriri, A. A. M., Chatrath, S. K., & Mohammadian, M. (2025). Exploring Determinants of Information Security Systems Adoption in Saudi Arabian SMEs: An Integrated Multitheoretical Model. *Journal of Cybersecurity and Privacy*, *5*(4), 113. https://www.mdpi.com/2624-800X/5/4/113.

Drescher, D. (2017a). *Blockchain Basics*. Springer. https://doi.org/10.1007/978-1-4842-2604-9.

Drescher, D. (2017b). Using the Blockchain. In *Blockchain Basics* (pp. 223-233). Apress. https://doi.org/10.1007/978-1-4842-2604-9.

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, *18*(1). https://doi.org/10.2307/3151312.

Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the association for information systems*, *4*(1), 7.

Hair, J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017). PLS-SEM or CB-SEM: updated guidelines on which method to use. *International Journal of Multivariate Data Analysis*, *1*(2), 107–123. https://doi.org/10.1504/IJMDA.2017.087624.

Hair, J. F., Sarstedt, M., Hopkins, L., & G. Kuppelwieser, v. (2014). Partial least squares structural equation modeling (PLS-SEM). *European Business Review*, *26*(2), 106–121. https://doi.org/10.1108/EBR-10-2013-0128.

Kaushal, P., & Khan, R. (2018). A Review on Information Security. *International Journals of Advanced Research in Computer Science and Software Engineering*, *8*(4).

Li, B., & Li, S. (2023). Research on Computer Data Security and Protection from the Perspective of Blockchain Technology Support. https://doi.org/10.26855/acc.2023.04.005.

Li, D., & Gong, Y. (2022). The design of power grid data management system based on blockchain technology and construction of system security evaluation model. *Energy Reports*, *8*, 466–479. https://doi.org/10.1016/j.egyr.2022.05.277.

Li, Y., Wen, Z., Hau, K.-T., Yuan, K.-H., & Peng, Y. (2020). Effects of cross-loadings on determining the number of factors to retain. *Structural Equation Modeling: A Multidisciplinary Journal*, *27*(6), 841–863. https://doi.org/10.1080/10705511.2020.1745075.

Liu, L., & Xu, B. (2018, 20-22 April 2018). Research on information security technology based on blockchain. 2018 IEEE 3rd international conference on cloud computing and big data analysis (ICCCBDA), Chengdu, China. https://doi.org/10.1109/ICCCBDA.2018.8386546.

Low, M. P., Ong, S. F., & Tan, P. M. (2017). Would internal corporate social responsibility make a difference in professional service industry employeesâ€ ™ turnover intention? A two-stage approach using PLS-SEM. *9*(1), 24.

Madanchian, M., & Taherdoost, H. (2025). A Narrative Review and Gap Analysis of Blockchain for Transparency, Traceability, and Trust in Data-Driven Supply Chains. *Applied Sciences*, *15*(17), 9571. https://www.mdpi.com/2076-3417/15/17/9571.

Manu, M., Musthafa, N., Balamurugan, B., & Chauhan, R. (2020). Blockchain components and concept.

McEvily, B., Zaheer, A., & Soda, G. (2021). Network trust. In *Understanding trust in organizations*. Taylor & Francis. https://doi.org/10.4324/9780429449185.

Merkow, M. S., & Breithaupt, J. (2014). *Information Security: Principles and Practices* (Second ed.). Pearson Education, Inc.

Mohamed, Z., Ubaidullah, N., & Yusof, S. (2018, October 2018). An evaluation of Structural model for Independent learning through connectivism theory and web 2.0 towards student achievement. International Conference on Applied Science and Engineering (ICASE 2018), https://doi.org/10.2991/icase-18.2018.1.

Monev, V. (2020, 17-18 Sept. 2020). Defining and Applying Information Security Goals for Blockchain Technology. 2020 International Conference on Information Technologies (InfoTech), https://doi.org/10.1109/InfoTech49733.2020.9211073.

Muhammad, S. A., Karim, M. A., & Kawthar, B. I. (2022). The role of Blockchain technology in enhancing the security of accounting information. *AL GHAREE for Economics and Administration Sciences*, 1701–1726.

O'brien, J. A. (1990). *Management information systems: A managerial end user perspective*. Richard D. Irwin, Inc.

Patel, V., Khatiwala, F., Shah, K., & Choksi, Y. (2020, 2020//). A Review on Blockchain Technology: Components, Issues and Challenges. ICDSMLA 2019, Singapore. https://doi.org/10.1007/978-981-15-1420-3_137.

Patricio, L. D., & Ferreira, J. J. (2021). Blockchain security research: Theorizing through bibliographic-coupling analysis. *Journal of Advances in Management Research*, *18*(1), 1–35. https://doi.org/10.1108/JAMR-04-2020-0051.

Pohl, M., Degenkolbe, R., Staegemann, D., & Turowski, K. (2020). *Towards a Blockchain Technology Frameworkâ€ "Literature Review on components in blockchain implementations* Australasian Conference on Information Systems2020, Wellington.

Raouf, A. A., & Raouf, M. A. (2022). *Information security basics.* Dar Al Masirah,.

Rizky, A., Kurniawan, S., Gumelar, R. D., Andriyan, V., & Prakoso, M. B. (2021). Use Of blockchain technology in implementing information system security on education. *4*(1), 62–70. https://doi.org/10.30743/best.v4i1.3640.

Roopnarain, M., & Mwapwele, S. D. (2025). Factors influencing the adoption and usage of blockchain in e-commerce: A systematic literature review. *African Journal of Science, Technology, Innovation and Development*, *17*(2), 238-251. https://doi.org/10.1080/20421338.2025.2459428.

Sabiri, K., Sousa, F., & Rocha, T. (2025). A systematic review of privacy-preserving blockchain applications in healthcare. *Multimedia Tools and Applications*, *84*(32), 39925-39980. https://doi.org/10.1007/s11042-024-20541-z.

Shaheen, S. K. (2020). Information Security "Editorial issue.". *Arab Journal of Informatics and Information Security*, *1*(1), 1–4. https://doi.org/10.21608/jinfo.2020.166263.

Shen, M., Zhu, L., & Xu, K. (2020). *Blockchain: Empowering Secure Data Sharing*. Springer. https://doi.org/10.1007/978-981-15-5939-6.

Shrier, D., Wu, W., & Pentland, A. (2016). Blockchain & infrastructure (identity, data security). *1*(3), 1-19.

Singh, A., Vaish, A., & Keserwani, P. K. (2014). Information Security: Components and Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, *4*(1).

Sr, S., N, U., R, C., & Cm, A. (2025). Comparison Between Encryption Algorithms: A Performance and Security Perspective. *International Journal on Science and Technology*, *16*(3). https://doi.org/10.71097/IJSAT.v16.i3.7986.

Subburaj, T., Raju, K. S., Suthendran, K., Kumar, K. P., Rekha, C., Sultana, S., & Deeraj, C. (2025, 28 February 2025). Biometric Authentication with Blockchain: A Secure and User-Friendly Approach. In V. S. Reddy, V. K. Prasad, J. Wang, & N. M. Rao Dasari, Intelligent Systems and Sustainable Computing Singapore. https://doi.org/10.1007/978-981-97-8355-7_44.

Suma, V. (2019). Security and privacy mechanism using blockchain. *Journal of Ubiquitous Computing and Communication Technologies*, *1*(01), 45–54. https://doi.org/10.36548/jucct.2019.1.004.

Taherdoost, H. (2022). Cybersecurity vs. information security. *Procedia Computer Science*, *215*, 483–487. https://doi.org/10.1016/j.procs.2022.12.050.

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), 15–17. https://doi.org/10.1145/2994581.

Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, *31*(2), 243–256. https://doi.org/10.1016/j.clsr.2015.01.005.

Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*, *13*, 32-39. https://doi.org/10.1016/j.jii.2018.07.004.

Xinyi, Y., Yi, Z., & He, Y. (2018). Technical characteristics and model of blockchain. 2018 10th international Conference on communication Software and networks (ICCSN), https://doi.org/10.1109/ICCSN.2018.8488289.

Zeng, Z., Li, Y., Cao, Y., Zhao, Y., Zhong, J., Sidorov, D., & Zeng, X. (2020). Blockchain Technology for Information Security of the Energy Internet: Fundamentals, Features, Strategy and Application. *Energies*, *13*(4), 881. https://doi.org/10.3390/en13040881.

Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. *ACM Computing Surveys*, *52*(3), 1–34. https://doi.org/10.1145/3316481.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. 2017 IEEE international congress on big data (BigData congress), http://www.doi.org/10.1109/BigDataCongress.2017.85.