International Journal of Studies in Business Management, Economics and Strategies
Volume 4, Issue 11, November- 2025
ISSN (E): 2949-883X
Scholarsdigest.org

EVALUATING THE EFFECTIVENESS OF BLOCK CHAIN TECHNOLOGY IN ENHANCING THE SECURITY OF DIGITAL FINANCIAL DATA: A CASE STUDY ON A SAMPLE OF COMMERCIAL BANKS OPERATING IN IRAQ

Ghaith Majid Hameed[1],
Kadhim Abed Leethan2
Audit and Internal Control Department /Wasit Education Directorate/ Wasit, Iraq
Email: Ghameed@uowasit.edu.iq,
kleethan@uowasit.edu.iq

Abstract
This study uses a case study of a sample of Iraqi commercial banks to assess how well block chain technology can improve the security of digital financial data. Since conventional security measures are no longer adequate, the study is crucial in addressing the pressing need to create security systems to thwart cyberattacks that jeopardize the integrity of digital financial data.
"There is a statistically significant effect of the effectiveness of block chain technology in protecting digital financial data," is the main hypothesis that the study tests. The deductive and inductive methods were used by the researchers, and a sample of forty-five employees of Al-Taif Islamic Bank and Al-Janoub Islamic Bank were used in the study.
The statistical findings support the alternative hypothesis by showing that block chain technology directly and significantly improves the security of digital financial data. Block chain characteristics, the independent variables, account for 81% of the variance in the dependent variable (digital financial data security), indicating that the model effectively depicts the phenomenon under study.
The results showed that the features of the technology, like immutability, which bars alteration and deletion, and decentralization, which prevents a system breach all at once, are a fundamental approach to security problems. By contrast, scalability is one of the primary barriers to the technology's implementation in banks.
The researchers advise banks to prioritize high-speed processing solutions to overcome the scalability issue and carefully incorporate blockchain technology into their current security infrastructure.

Keywords: Block chain technology; Digital financial data security; Commercial banks; Iraq; Financial security; Case study; Banking sector; Data integrity.

Introduction

The modern global economy is now built on digital transformation, as digital financial data has emerged as the most important strategic asset for economic entities in general and the banking sector in particular. Because the commercial banking sector currently relies so heavily on digital systems, these systems are vulnerable to cyberattacks and are at significant risk. The security and integrity of this data are now in jeopardy because of their susceptibility to cyberattacks, which could lead to significant financial losses and a reduction in the trust that customers have in these businesses.

Traditional financial data protection methods like firewalls and antivirus software are insufficient to handle modern threats. Because of this, there is now a greater need to develop data security systems. High levels of security, transparency, and dependability can be provided by decentralized, encrypted block chain technology in a setting where data is not trusted.

Block chain technology's decentralization and immutability make it an essential solution for security problems in the banking sector. This prevents fraud and manipulation because no record or transaction added to the chain can be taken out or changed. Additionally, the distribution of records among many participants eliminates the potential for a system-wide hack.

The researchers noted that although there is interest in integrating block chain technology into global financial systems, there is still a lack of research on its potential applications in Iraq. This is due to a number of barriers to its adoption, such as those related to digital readiness, infrastructure, and legal requirements.

Thus, this research attempts to close the knowledge gap that might prevent the assessment of how well block chain technology protects the security of digital financial data and improves its dependability. This is accomplished by using a case study of a subset of Iraqi commercial banks. Drawing from the aforementioned, the researchers will investigate the ways in which this technology affects and its capacity to create a safe and dependable banking system that can withstand any threats.

Chapter One: Research Methodology and Previous Studies

1. Research methodology

The following is a presentation of the research methodology, which includes the research problem, its objectives, importance, hypothesis, spatial and temporal limits of the research, and sources of data collection, according to the paragraphs shown below:

1.2. Research problem

Professionals (accountants and auditors) began to wonder whether block chain technology would threaten their jobs or replace them. However, many ultimately concluded that this technology would contribute to the development of the accounting profession and reduce many repetitive accounting practices. It is important to learn how this technology works before it becomes part of their daily work. Accountants do not need to be engineers with full knowledge of how block chain technology works, but they simply must have knowledge of how it works, expand their skills, and be able to understand its functions and principles. For

these reasons, the world's largest accounting firms have turned to exploring block chain applications to better serve their clients and achieve a competitive advantage. (Abdul Hamid, 2021: 4)

The research problem is embodied in the digital financial data and providing security for this data, as the more protection means there are, the more reliable the financial data becomes (a direct relationship) in light of the effectiveness of block chain technology and the benefits thereof. The research problem can be formulated in light of the following questions:

1.2.1. What is block chain technology and how does it work?

1.2.2. What are the challenges facing the implementation of block chain technology in banks?

1.2.3. To what extent does block chain technology affect the protection of digital financial data?

1.3. The importance of research

The researchers think that because block chain technology has inherent qualities that make it impervious to fraud and manipulation, it is evidently effective in improving the security of digital financial data. Because it demonstrates how the properties of the technology can be used to secure financial systems, this study is significant because it increases user trust in digital financial data due to its fundamental principles (decentralization, encryption, transparency, and immutability). Additionally, this research is significant because of the following factors:

1.3.1. In a context where data mistrust is increasing due to fraud and cybercrime, the study adds to our understanding of how block chain technology can increase users' confidence in digital financial transactions.

1.3.2. Applying block chain technology to financial system problems like safeguarding external payments and managing digital assets may be made easier by the study's novel ideas.

1.3.3. The research findings can be used by policymakers to better understand block chain technology and develop laws and regulations that promote its safe and effective use in the banking sector.

1.3.4. The development of financial technologies and cybersecurity is made possible by research, which opens up new possibilities for the development of safer and more efficient financial systems.

1.4. Research objectives

Given the following, the primary objectives of this study are to provide a comprehensive understanding of how this technology improves current security systems and to identify any possible issues with its use:

1.4.1. Gain an understanding of the technology's decentralized encryption and verification mechanisms, and assess how well it guards against financial data manipulation or distortion once transactions have been recorded.

1.4.2. Identify and evaluate the challenges and risks that hinder the implementation of this technology, such as (scalability and energy consumption).

1.4.3. Providing practical recommendations to banks on how to integrate this technology into their security infrastructure and proposing measures to simplify the transition to a secure digital transformation.

1.5. Research hypothesis

Main Hypothesis: There is a significant impact of the effectiveness of blockchain technology in protecting digital financial data.

1.6. Temporal and spatial limits of the research

Below we show the temporal and spatial boundaries of the research as shown below:

1.6.1. Timeframe: Data from a number of commercial banks listed on the Iraq Stock Exchange for the year 2025 is used to focus on banks' future plans for adopting this technology and the possibility of its implementation.

1.6.2. Spatial boundaries: The spatial boundaries of the research are limited to a sample of private commercial banks in Iraq listed on the Iraq Stock Exchange.

1.7. Research methodology and data sources

To achieve the previously set objectives, the deductive and inductive approaches will be followed, where we will explain the sources of all data according to the two approaches, as shown below:

1.7.1. Deductive approach: To enrich the theoretical aspect of the research, we will rely on the contributions of researchers and writers on the topic of our research, which will be collected from published scientific sources (Arabic and foreign), as well as periodicals, master's theses, doctoral dissertations at universities, and studies and articles published on the Internet.

1.7.2. The inductive approach: This approach was adopted in the applied aspect of the research, and we relied on a set of methods to obtain data that would help achieve the research objectives. These methods include field meetings and personal interviews with the individuals responsible for the research sample.

1.8. Previous studies

Below we list a number of previous studies (Arab and foreign) that are relevant to the topic of our research, as follows:

1.8.1. Arabic studies:

Table No. (1)

the details	
1	**Study (Abdul Hamid, 2021)**
Research title	"The impact of using blockchain technology on the accounting environment in Egypt"
Research type	Theoretical field study.
Research objectives	Learn about blockchain technology, its working mechanism, advantages, experiences with its use, and its relationship to the accounting business environment. Explain the challenges facing the implementation of this technology and demonstrate the success of accounting systems that have used it.
Results	This technology's implementation is fraught with challenges, chief among them being operational risks, governance problems, and the lack of accounting systems. This field is impacted as well, given the changing nature and extent of the accounting and auditing profession.
2	**Study (Ismail, 2021)**
Research title	"Block chain technology is a mechanism for the governance of contemporary Islamic financial institutions"
Research type	Theoretical study.
Research objectives	Gain a thorough understanding of blockchain technology, including its functions, uses, and benefits. Gain insight into the special characteristics that make it a comprehensive tool for overseeing modern financial institutions.
Results	Block chain technology holds promise for a new era of governance for Islamic financial institutions, one based on sound judgment, accurate financial data, and fair transactions based on accepted principles. System problems and employee resistance have prevented this technology from gaining the widespread acceptance that would allow it to be used in a variety of industries.
3	**Study (Kentash, 2025)**
Research title	"Smart contracts integrated into the digital block chain are a tool for stimulating foreign trade and improving the performance of the banking system"
Research type	Descriptive analytical study.
Research objectives	Learn the fundamentals of smart contracts, which are related to block chain technology and can be used to boost global trade and the effectiveness of the banking system. Analyze the compatibility of smart contracts and block chain technology, and emphasize the importance of educating the public about the state-of-the-art financial technology industry.
Results	The study concluded that it is essential to use this technology due to its efficiency, transparency, and decentralization. Building a new financial system that is more technically and legally feasible is another goal, as is creating an index to evaluate the standing of global commercial organizations.

1.8.2. Foreign studies:

Table No. (2)

the details	
1	**Study (Omolara, Temitayo, and Paschal, 2024)**
Research title	"Encryption Techniques for Financial Data Security in FinTech Applications"
Research objectives	pointing out how crucial it is to safeguard the confidentiality and integrity of financial data, how crucial encryption is to financial data cybersecurity and the dangers of cyberattacks, how to prevent unauthorized access and hacking, and how advanced encryption helps safeguard financial data.
Results	One example of symmetric encryption that offers good data protection and is appropriate for safely storing digital data and handling transactions in real time is the Advanced Encryption Standard (AES). These technologies are compatible with asymmetric encryption, like ECC and RSA. In order to increase the security and effectiveness of the encryption process, hybrid encryption technologies combine the advantages of symmetric and asymmetric encryption. These safeguards aid in the protection of private financial data on a variety of fintech platforms, such as cryptocurrency trading platforms, online banking portals, and mobile payment apps. It is impossible to exaggerate the importance of encryption in fintech. In addition to safeguarding financial data from unwanted access, it also fosters user confidence, encourages adherence to regulations, and fosters innovation in online financial services.
2	**Study (Man and Soojin, 2021)**
Research title	"Financial Consumer Protection in the Age of Digital Transformation"
Research objectives	This study's primary goal is to identify best practices in financial consumer protection policies by developing the essential components of a welfare-enhancing system of financial consumer protection policies. It focuses on three main pillars: financial education, ex-ante (or pre-point of sale) financial consumer protection measures, and ex-post policy tools.
Results	Any financial consumer protection policy regime should aim to achieve two behavioral outcomes: financial consumers making wise and informed decisions and financial institutions and their staff treating customers fairly and ethically. Each of the three pillars covered in this manuscript ought to help achieve this.

1.9. Differences between the current study and previous studies

The researchers believe that our study differs from the previous studies above in that our study does not only aim to examine the existence of block chain technology, but also to measure the performance of this technology and its effectiveness in protecting digital financial data. Previous studies were more general, as some focused on the (accounting environment), some on the administrative and regulatory side, and others on the economic and commercial side. The title of our study focused directly and specifically on the security

of digital financial data, which is a very vital topic, as protecting customer and transaction data is a top priority in the banking sector. "Encryption Techniques for Financial Data Security in FinTech Applications" (Omolara, Temitayo, Paschal, 2024) is a topic close to our study, but it is broader in scope (financial technology) and narrower in focus (encryption) than using block chain technology as a comprehensive security system to enhance digital data security.

On the other hand, our studies focus on private commercial banks operating in Iraq and listed on the Iraq Stock Exchange. This geographical focus is a key strength, as the effectiveness of any technology depends largely on the regulatory and legal environment and local infrastructure. Studying the impact in the context of a specific country, such as Iraq, adds direct practical and applied value to the research. Previous studies, however, address broader or entirely different geographic areas. This diversity makes our study unique in its focus on the challenges and opportunities available in Iraq.

Chapter Two: The Conceptual Framework

1. Knowledge foundations of block chain technology and its definitions

Due to the technological developments witnessed by the whole world, the future will belong to those who adopt digital technologies, which may force economic units to change their working methods in all fields. Block chain technology is one of the most important and newest of these technologies that can be used in all sectors, as this technology is the basic component of digital currencies. The World Economic Forum predicted that during this year (2025), the global GDP will depend on block chain technology by a percentage of no less than 10%, and by 2030, the global GDP from block chain technology will reach $3.1 trillion in business value (Abdul Halim, et al., 2025: 107). This technology has the great potential to impact all aspects of our lives, as it can complete payment and settlement transactions from days to a few seconds, increase information security rates, and significantly reduce administrative service costs. Commercial licenses and permits can also be issued for companies within minutes instead of days (Abdul Hamid, 2021: 8). Block chain is a term composed of two words (chain - Record) meaning that the digital information stored is in a sequential manner within the records of the general database distributor through algorithms. This technology went through four stages, and each stage has its own goals and advantages: (Kentash and Hashman, 2025:70)

1.1. First Generation: This phase aims to improve the monetary system (payments and transfers, stock speculation, and simple smart contracts). The primary platform for this phase (mining, encryption, and public ledger) and its application are linked to cryptocurrency, as this phase is linked to digital transformation.

1.2. The second Generation: This is the stage of smart contracts, which includes cryptocurrencies, digital identity management, complex exchange management, and electronic records management. This stage represents the transition to a digital economy.

1.3. Third Generation: This phase featured the distributed (decentralized) ledger, internet currency, distributed ledgers based on lattice, decentralized management, e-governance systems, and the use of applications that combine user-friendly interfaces with smart contracts, integration between systems, and the use of artificial intelligence technologies.

1.4. Fourth Generation: The goal of this generation is to incorporate block chain technology into current business procedures. It depends on using artificial intelligence technologies to create a more resilient infrastructure that can handle sophisticated applications and high transaction volumes.

(Abdul Hamid, 2021:9) defined block chain technology as a database in the form of a distributed ledger that records all digital financial transactions and stores them in sequential, encrypted blocks that no one can hack or modify and that are available to network members via millions of computers connected to the Internet.

(Aliwa and Wasil, 2025:47) see the definition of block chain technology as a digital ledger of accounts distributed and shared between multiple parties through which financial transactions can be recorded at the time of their occurrence in a way that ensures security, transparency and decentralization, as there is no central authority to control or manipulate the data, which makes this data different from traditional data, as the process of recording in its historical time makes it not subject to modification or manipulation and distinguishes it with transparency, reliability, efficiency and speed in completing transactions, whether internal or external transfers and other financial transactions.

(Al-Naqeeb and Abdel-Azeem, 2024:12) defined it as a system that allows a group of computers to create a central digital ledger to verify, save and authenticate transactions and data in a large chain of encrypted data on millions of points called “contracts”, allowing many parties to enter and verify information, as each point, computer or entity in the chain has the same copy of this data and information, as all contracts, agreements or information are added to the chain and verified before being added according to the mechanism followed in block chains, which ultimately provides a public, encrypted and secure record that no one can modify or tamper with.

A network of linked computers with safe, encrypted data that promotes security and decentralization is what the researchers refer to as block chain technology. This technology is designed to preserve data without modification, meaning that when any information is added to it, no one can modify it. The goal of this technology is to eliminate the need for a third party (intermediary), which leads to building trust between the two parties and completing all transactions without the intervention of any other person.

2. How does blockchain technology work?

Blockchains are a fast accounting system that saves all the transactions disclosed by the participants in the block chain, which consists of a group of blocks starting with the creation block, which is the first stage of each chain. These blocks are linked together through links called nodes, as one block consists of a group of transactions. These transactions are made up of the sender and the recipient, and the information of that transaction is secured through the encryption code, from which the block chain derives an important and distinctive element,

which is the element of trust between the participating parties. This technology is distinguished by its use of encryption codes and mathematical algorithms that ensure the accuracy of the recorded information and the impossibility of tampering. The process of displaying and recording that data consists of five main steps: (Muhammad, 2025: 324)

2.1.Transaction definition: The sender creates a transaction containing information (recipient's address, transaction value, encrypted digital signature that verifies the accuracy of the transaction).

2.2.Transaction Authentication: The message is momentarily suspended for use in building the block when nodes in the network receive a transaction. They do this by opening the pre-installed digital signature code to confirm the message's legitimacy.

2.3. Block creation: To update the ledger or block, one of the network's nodes uses the pending transaction. Other nodes are notified of the updated block after a predetermined amount of time so they can wait and confirm the data.

2.4. Block validation: When the nodes in charge of network verification receive a request to validate the updated block, they must go through a tedious procedure that necessitates other nodes' approval.

2.5. Block Chaining: When the nodes in charge of network verification receive a request to validate the updated block, they must go through a tedious procedure that necessitates other nodes' approval.

The researchers conclude that block chain technology provides increased security for participant transactions, as well as verifying the validity of transactions that arise by unlocking the codes of the pre-established digital signature. Also, when a block is created, nodes publish the new blocks to others to verify their validity. This process guarantees that the information is accurate. The audit process is repeated after the updated blocks' validity has been confirmed, and the other blocks' approval for the update is asked for. Then, using a digital process free from outside intervention, the block's new state is published to the other blocks, guaranteeing security and protecting data inside the blocks. Keep in mind that the five steps listed above only require ten seconds or less.

3. Challenges Facing Block chain Technology in Banks

Blockchain technology has the potential to revolutionize the banking industry. But there are many obstacles in the way of its implementation, such as the absence of a worldwide standard for blockchain technology. Security is another issue for banks that use this technology because there is no clear legal or security framework for it, nor is there any international law that governs it. One of the largest challenges for banks utilizing this technology is scalability, which they must be ready to handle (Gyimah et al., 2023: 37). Transactions become slower and more costly as the network processes more of them. For instance, the Bitcoin network can process seven transactions per second, whereas the Visa network can process twenty-

four thousand transactions per second (Aliwa and Wasil, March, 2025: 49). Block chains in banks also face difficulties because traditional banking systems were not built to accommodate block chain technology, and banking systems still rely on antiquated technologies to carry out their operations. Many international players using a variety of technologies are commonly found in the financial market ecosystem. Global efforts are currently being made to create block chain systems. Since block chain systems are often developed in isolation and with disparate methodologies and technologies, it can be difficult to integrate them so they can communicate effectively and seamlessly. Cross-border payments and remittances, which necessitate that funds travel through several nations, present a bigger challenge. Moreover, the integration of block chain technology, a decentralized technology, into traditional payment systems, which depend on a centralized mechanism, complicates matters considerably, particularly when decentralized systems are anticipated to depend on the centralized mechanism already in place. (Mafike, & Mawela, 2022:13)

The researchers dispute the idea that block chains lack a legal framework, asserting that the transparency this technology offers reduces regulatory risks by aiding in adherence to laws such as those governing anti-money laundering and counterterrorism financing. They agree that scalability concerns are a significant obstacle for banks that must process a large number of transactions rapidly and effectively.

4. Block chain technical characteristics

The unique ability of block chain technology to create security and trust in decentralized business environments stems from its interconnected features. Five main dimensions can be used to summarize these salient characteristics that distinguish this technology from traditional databases: (Vaigandla and others, 2023:77).

4.1. Immutability: The inability to change data, or immutability, is undoubtedly one of the most remarkable aspects of blockchain technology. This technology's most important feature is its capacity to build an unalterable, permanent network. The immutability of block chains means that data cannot be changed. The data must also be authorized by each network node before being added to the block in order to facilitate secure transactions.

4.2. Decentralization: Each transaction must be validated by a central authority in traditional centralized transaction systems, which can be expensive and performance-intensive. Nevertheless, block chain technology lacks a governing body and a single organization in charge of the framework. Decentralized networks are characterized by the fact that they are run by a collection of nodes, or computers. Since the data is spread across several nodes rather than a single central server, hacking is challenging. It also allows participants to communicate directly with one another, which reduces costs and increases efficiency.

4.3. Permanence: Transactions are quickly verified. Once added, a transaction cannot be removed from the block chain or undone. Blocks can be immediately examined for anomalous transactions. Since any transaction or block can be verified thanks to the structure

of the block chain, data stored in the chain is permanent and traceable. It allows for a complete history of all currencies by providing each node with a single record of all Bitcoin transactions. Double-spending is addressed by this feature.

4.4. Confidentiality: The encryption of subscribers' addresses hides their real identities. This blends the ability to track transactions (transparency) with the privacy of the real identities of the trans actors.

4.5. Auditability: This system enables efficient fraud detection and transaction tracking. The block chain allows for easy tracking and verification of data because each transaction is time-stamped and verified. Information is thus kept clear, traceable, and verifiable. These records are accessible to all network users via computer algorithms that guarantee the distributed ledger's chronological order and permanence.

5. Digital Financial Data Concept

It is developed using financial technology and security literature, with an emphasis on form, because there isn't a single, consistent definition of digital financial data in accounting standards. As per the BIS (2023), it is characterized as "any financial information that is generated, processed, transmitted, and stored electronically in an intangible form." Because it is the raw material that embodies the unit's economic phenomena—such as purchasing, selling, transferring, and other transactions—in an intangible form, this data is extremely important (IASB, 2018). High security measures must be implemented as a result in order to guarantee the stability of these units' financial systems. (FSB, 2024).

The researchers believe that the BIS represents the technical source for defining the digital form of financial data within modern systems, the FSB represents the source that confirms the security importance of digital data and its connection to financial stability, and the IASB represents the accounting source that determines the content (economic phenomena) and purpose of this data.

Digital transformation in the financial sector is defined as the process by which digital technology is used to transform traditional financial services into advanced services, enabling easy access to them via mobile applications and the internet. This includes the use of electronic systems and artificial intelligence tools to provide better services to customers, reduce the cost of financial services, and increase efficiency (Naimi-Sadigh et al., 2022: 1212).

6. Elements of digital financial data security

In order to protect financial data from attacks, a series of elements must be available. Ahmed divided these elements into five: (Ahmed, 2021: 261)

6.1. Confidentiality: It is a fundamental principle in digital financial data that refers to the protection of sensitive financial and personal information of individuals and economic units from unauthorized access, improper use, modification, or disclosure, and ensuring that this data is available only to authorized parties. This data includes information such as (bank

account numbers, transaction details, credit history, payment card data, and financial records), and the importance of confidentiality increases with the digital transformation and the increasing reliance on online financial services.

6.2. Identity verification: This means verifying the identity of the person conducting the financial transaction and determining whether or not it is the same person. This is done through a secret code specific to each user. The RAS organization explains three methods for identity verification: things that the person knows, such as the password, the code that the user enters into the personal computer to obtain operating permission, fingerprints, face, or voice.

6.3. Content integrity: This means ensuring that the content of financial data is secure and will not be altered or corrupted at any stage of data processing, whether the processing is inside the unit or outside it by an unauthorized person, usually resulting from illegal intrusions such as viruses. No one can corrupt the data or change the account balance. Therefore, the financial institution is responsible for ensuring the security of the content through preventive measures (such as technologies, programs, or anti-virus equipment).

6.4. Availability: This means ensuring that the system and all its components continue to operate properly, as well as the ability to interact with information and provide the necessary services on time, as well as preventing illegal use.

6.5. Non-repudiation According to this principle, no one participating in a digital transaction or process can subsequently claim that they did not carry out that action or process. Therefore, it must serve as proof for anyone carrying out a specific transaction, like confirming an electronic identity or using an electronic signature.

7. The relationship between the characteristics of block chains and the dimensions of financial data security

The conceptual framework of the study is defined by the fundamental relationship between the independent and dependent variables as revealed by examining their theoretical foundations. Block chain technology's attributes, as an independent variable, reflect the collection of cognitive underpinnings believed to have a direct and positive impact on the aspects of digital financial data security, while the dependent variable is the technology itself. This relationship is based on the fact that the special characteristics of block chains—their immutability, decentralization, confidentiality, and auditability (Vaigandla et al., 2023:77)—act as technological instruments designed specifically to enhance the security requirements of the financial sector (Ahmed, 2021:261). For example, once transactions are recorded and encrypted in the block, the immutability principle ensures the integrity of the data and makes it nearly impossible to tamper with them. Decentralization also improves availability by reducing the likelihood of disruption from a single central point of failure through the distributed ledger across millions of nodes. It also makes identity verification easier by utilizing digital signatures. The features of block chain offer a structural means of enhancing

security and transparency in the banking sector, notwithstanding scalability concerns (Gyimah et al., 2023; Mafike & Mawela, 2022). In 2025, Aliwa and Wasil and Abdul Halim et al.

As a result, the researchers can assess how well this technology satisfies the fundamental security requirements (availability, integrity, confidentiality, and identity verification) in compliance with contemporary academic frameworks. The conceptual framework of the study is founded on a model that evaluates the degree to which the independent variable (blockchain characteristics) influences the dependent variable (financial data security dimensions). (Warkentin & Orgeron, 2020).

Chapter Three: Practical Aspect

1. Iraqi banks listed on the Iraq Stock Exchange (study population)

The Securities Commission is a supervisory body that regulates the capital market. It was established pursuant to Law No. (74) of 2004. The aim of establishing this commission was to protect investors in securities and to regulate and develop the capital market continuously to achieve justice, efficiency and transparency and to protect this market from potential risks. The affairs of this commission are managed and supervised by a board consisting of five commissioners, including a chairman and two deputies, provided that the chairman and deputies are dedicated to working in this commission (full-time). The remaining members are part-time, provided that they have experience and expertise. This board has multiple tasks to achieve its established objectives, including preparing draft laws and regulations, issuing instructions and regulations related to capital markets, granting licenses to financial markets and brokerage firms, and approving the listing of securities in the capital market.

Our study community represents two banks listed in the Iraq Stock Exchange, namely (Al-Tayf Islamic Bank and Al-Janub Islamic Bank). In light of the modest capabilities of the researchers and based on the practical and statistical determination of the sample size, a random sample of employees in these two banks was selected to form a community to test the study hypotheses, as the size of this sample reached (45) people, as we found that the banking sector is the appropriate sector to evaluate the effectiveness of blockchain technology in enhancing the security of digital financial data.

2. An introductory overview of the Islamic Bank of the South and the Islamic Spectrum Bank

Below is an introductory summary of the study community, which is represented by (South Islamic Bank and Al-Tayf Islamic Bank), which are listed on the Iraq Stock Exchange.

2.1. Islamic Bank of the South

It is one of the private Iraqi banks listed on the Iraq Stock Exchange. It was established in 2016 by a group of businessmen specialized in the fields of agriculture, food, financial investments, and other industrial projects. This bank was established to meet the needs of the Iraqi financial market in accordance with Islamic Sharia. The bank also provides a number of financial and banking services targeting the individual and economic sectors. Its paid-up capital amounts to 250 billion Iraqi dinars.

2.2. Al-Tayf Islamic Bank

It is one of the private Iraqi banks listed on the Iraq Stock Exchange, where it was initially established as a joint-stock company in 2006 with a capital of (85,000) US dollars. In late 2018, the company was converted into a bank, where the articles of association were amended and its activity was changed to practicing banking business according to the Islamic method. It began practicing banking business in 2019 within (13) branches, (4) of which are in Baghdad and the rest are distributed among the governorates. The bank also seeks to expand its services within the limits of a future plan to open branches in all Iraqi governorates.

3. Display, analyze and interpret research results

The arithmetic mean, standard deviation, percentage, and sample trend for the paragraphs were utilized in the following manner to ascertain the responses of the study sample members with respect to the primary paragraphs contained in the study tool:

3.1. Arithmetic mean: This is to assess how well or poorly each study paragraph was received by the participants.

3.2. Standard Deviation: to determine how far the study participants' responses to each paragraph deviate from the study's arithmetic mean. It should be noted that in addition to the main axes, the standard deviation displays the dispersion in the study participants' responses to the paragraphs. The answers are less scattered across the scale and more concentrated when their value is near zero.

3.3. Calculating the range: Here, the value on the five-point Likert scale is (largest value - smallest value). (5-1=4).

3**.4. The cell length** is calculated by dividing the number of Likert scale fields by the range., (4/5=0.80).

3.5. The cell's upper limit (I strongly disagree) is then obtained by adding the cell length to the scale's smallest value, (1). This process continues until we reach each cell's lower and upper limits, which are as follows:**3.5.1.** Any mean value between (1-1.79) is classified in the cell (strongly disagree). This represents a percentage of less than (20%).

3.5.2. The cell (I disagree) classifies any arithmetic mean value higher than 1.80 and up to 2.59. This indicates a percentage in the range of 21% to 40%.

3.5.3. Any mean value up to 3.39 and above 2.60 is categorized as neutral. This is a percentage that falls between 41% and 60%.

3.5.4. In the cell (agree), any arithmetic mean value higher than 3.40 and up to 4.19 is categorized. This is a percentage that falls between 61% and 80%.

3.5.5. According to Table No. (3), any arithmetic mean value higher than 4.20 and up to 5 is categorized in the cell (strongly agree), creating a percentage of more than 81%.

Table No. (3), statement of the scale of answers.

degree	1	2	3	4	5
Classification	I strongly disagree	I disagree	neutral	agree	strongly agree
Range	1-1.79	1.80-2.59	2.60-3.39	3.40-4.19	4.20-5
ratio	20%	40%	60%	80%	80-100%

3. Description of the research sample's responses to the dimensions of block chain technology

4.1. Stability property: The arithmetic mean of the first dimension (stability), according to the statistical results, was 3.67, higher than the hypothetical mean (3). On the other hand, the standard deviation shows that the opinions of the research sample are homogeneous. It reached 0.77 with a percentage of 73.4%, indicating that the sample is trending towards agreement, which shows that the research sample agrees with the paragraphs of the first dimension. The analytical description of the first dimension's paragraphs, as displayed in Table No. (4), is as follows:

Table (4) shows the statistical results (arithmetic mean, standard deviation and percentages)

Paragraphs	arithmetic mean	standard deviation	percentage	Sample orientation
1	3.83	0.7	76.6	I agree
2	3.63	0.72	72.6	I agree
3	3.59	0.76	71.8	I agree
For the first dimension as a whole	**3.67**	**0.77**	**73.4**	**I agree**

The table was prepared by the researcher using SPSS 1.0.

4.1.1. An examination of the opening paragraph: The arithmetic mean for paragraph No. (1), which concludes that "the nature of block chains provides absolute stability for financial records, as it prevents change or deletion after registration," is 3.83, which is higher than 3.40 and lower than 4.19. This suggests that the sample believes that the statement is true. In order to determine how far the responses of the participants in paragraph (1) deviate from the arithmetic mean, it is observed that the standard deviation is (0.7), indicating that the responses are less scattered and more uniform. The 76.6% percentage suggests that the sample is moving toward agreement.

4.1.2. Analyzing the second paragraph For paragraph No. (2), which asserts that "the stability property is more effective in preventing tampering with records compared to current central databases," the arithmetic mean is 3.63, which is lower than 4.19 and higher than 3.40. This implies that the sample accepts the statement as true. The degree of deviation of individual responses to paragraph (2) from its arithmetic mean can be ascertained by using the standard deviation of 0.72, which suggests that the sample is less dispersed and more homogeneous, and the percentage of 72.6%, which suggests that the sample leans toward agreement.

4.1.3. Analysis of the third paragraph: The sample's belief in the validity of paragraph No. (3), which states that "constancy ensures the creation of a reliable history of financial transactions that cannot be denied," is indicated by an arithmetic mean of (3.59), which is higher than (3.40) and lower than (4.19). With a standard deviation of 0.76, the participants'

answers to paragraph (3) show a degree of deviation from the arithmetic mean that is less dispersed and more consistent. The percentage, which is 71.8%, suggests that the sample tends to concur.

4.2. Decentralization feature: The arithmetic mean of the second dimension, or the decentralization characteristic, was 3.42, higher than the hypothetical mean (3), according to the statistical results. However, because the standard deviation reached (0.84) with a percentage of (68.4%), it shows that the research sample's opinions are homogeneous. This means that the sample's trend is towards (agree), which indicates that the research sample agrees with the paragraphs of the second dimension. According to Table (5), the second dimension's paragraphs are analytically described as follows:

Table (5) shows the statistical results (arithmetic mean, standard deviation and percentages)

Paragraphs	arithmetic mean	standard deviation	percentage	Sample orientation
1	3.49	0.77	69.8	I agree
2	3.29	0.89	65.8	neutral
3	3.54	0.8	70.8	I agree
For the second dimension as a whole	**3.42**	**0.84**	**68.4**	**I agree**

The table was prepared by the researcher using SPSS 1.0.

4.2.1. Examining the opening paragraph: Since the arithmetic mean for paragraph No. (1), which reads, "Distributing the record over multiple nodes reduces the possibility of the banking system malfunctioning (single point of failure)," was 3.49, higher than 3.40 and lower than 4.19, it is clear that the sample believes this statement to be true. The percentage reached (69.8%), indicating that the sample's tendency is towards (agreeing), and the standard deviation reached (0.77), indicating that the responses of individuals to paragraph (1) did not deviate significantly from their arithmetic mean.

4.2.2. Analysis of the second paragraph: Paragraph No. (2), which states that (decentralization supports the continuous availability of financial data services even if some nodes are hacked or damaged), has an arithmetic mean of (3.29), which is greater than (2.60) and less than (3.39), indicating that the sample has a (neutral) view of this statement. To identify the extent of deviation of individuals' responses to paragraph (2) from its arithmetic mean, it is noted that the standard deviation is (0.89), meaning that it is less dispersed and more homogeneous, and the percentage is (65.8%), which means that the sample's tendency is towards (neutral).

4.2.3. Interpretation of the third paragraph: An arithmetic mean of (3.54), which is higher than (3.40) and lower than (4.19), indicates that the sample views paragraph No. (3), which states that (decentralization contributes to reducing dependence on the sole central authority in verifying the validity of transactions), as (agreeing). The standard deviation was (0.8), indicating that the responses of the participants to paragraph (3) were less dispersed and more

homogeneous, indicating the degree of deviation from the arithmetic mean. Given that the percentage is 70.8%, the sample has a tendency to agree.

4.3. Confidentiality feature: The third dimension, or the confidentiality feature, had an arithmetic mean of 3.65, according to the statistical results, which is higher than the hypothetical mean (3). However, the standard deviation shows that the opinions of the research sample are homogeneous, reaching 0.79 with a percentage of 73%. This indicates that the research sample agrees with the third dimension's paragraphs and that the sample's trend is towards agreement. According to Table No. (6), the third dimension's paragraphs are analytically described as follows

Table (6) shows the statistical results (arithmetic mean, standard deviation and percentages)

Paragraphs	arithmetic mean	standard deviation	percentage	Sample orientation
1	3.49	0.89	69.8	I agree
2	3.78	0.68	75.6	I agree
3	3.76	0.73	75.2	I agree
For the third dimension as a whole	**3.65**	**0.79**	**73**	**I agree**

The table was prepared by the researcher using SPSS 1.0.

4.3.1. Interpretation of the opening paragraph: The arithmetic mean of paragraph No. (1), which reads, "The use of advanced encryption ensures that sensitive data is not exposed to unauthorized persons," was 3.49, which is higher than 3.40 and lower than 4.19. This suggests that the sample believes that the statement is true. The percentage is 69.8%, indicating that the sample has a tendency toward agreement, and the standard deviation was 0.89, indicating that the responses of individuals to paragraph (1) deviate from the arithmetic mean to a greater degree.

4.3.2. Making sense of the second paragraph: The arithmetic mean of 3.78, which is higher than 3.40 and lower than 4.19, indicates that the sample considers paragraph No. (2) to be (agreeing). According to the statement, "The blockchain's digital signature system helps to finally verify the sender's identity." The standard deviation was 0.68, suggesting that people's answers to paragraph (2) differ more from the arithmetic mean, while the percentage of 75.6% suggests that the sample has a tendency toward agreement.

4.3.3. The third paragraph's interpretation: The sample believes that confidentiality helps protect the identity of clients and the specifics of the financial transaction in the public record (if any), as stated in paragraph No. (3), with an arithmetic mean of 3.76, which is higher than 3.40 and lower than 4.19. It is noted that the percentage is 75.2%, suggesting that the sample has a tendency toward agreement, and the standard deviation was 0.73, suggesting that people's answers to paragraph (3) deviate less from the arithmetic mean.

4.4. Auditability feature: The statistical findings show that the fourth dimension (the property of auditability) had an arithmetic mean of 3.68, higher than the hypothetical mean (3). However, the standard deviation, which reached 0.8 and a percentage of 75.2%, suggesting that the sample's trend is towards (agree), shows that the research sample agrees with the paragraphs of the fourth dimension. The analytical description of the fourth dimension's paragraphs, as displayed in Table No. (7), is as follows:

Table (7) shows the statistical results (arithmetic mean, standard deviation and percentages)

Paragraphs	arithmetic mean	standard deviation	percentage	Sample orientation
1	3.44	0.77	69.8	I agree
2	3.29	0.89	65.8	neutral
3	3.83	0.7	76.6	I agree
For the fourth dimension as a whole	**3.68**	**0.8**	**75.2**	**I agree**

The table was prepared by the researcher using SPSS 1.0.

4.4.1. Interpretation of the opening paragraph: The arithmetic mean of paragraph number one, which reads, "Blockchain technology allows immediate and transparent tracking of the entire path of any previous financial transaction," was 3.44, which is higher than 3.40 and lower than 4.19. This suggests that the sample believes that the statement is true. The percentage is 69.8%, indicating that the sample's trend is towards agreement, and the standard deviation was 0.77, indicating that the responses of individuals to paragraph (1) deviate from the arithmetic mean to a greater degree.

4.4.2. Interpretation of the second paragraph: The sample's arithmetic mean for paragraph No. (2), which reads, "The ability to audit contributes to identifying the source of errors or fraud immediately and more efficiently," is 3.29, which is greater than 2.60 and less than 3.39. This implies that this statement is regarded as (neutral) by the sample. The sample has a tendency toward neutrality, as indicated by the percentage of responses to paragraph (2) of 65.8% and the standard deviation of 0.89, which shows that the responses are more homogeneous and less scattered. These results show how far the responses deviate from the arithmetic mean.

4.4.3. Interpretation of the third paragraph: The sample views paragraph No. (3), which states that "the presence of the open auditing record feature increases internal and external accountability in the bank," as "agreeing," as indicated by its arithmetic mean of 3.83, which is higher than 3.40 and lower than 4.19. The percentage is 76.6%, indicating that the sample has a tendency toward agreement, and the standard deviation arrived at 0.7, indicating that the responses of individuals to paragraph (3) deviate from the arithmetic mean to a greater degree.

4.5. Description of the responses to the research sample: The statistical results show that the second axis (digital financial data security) had an arithmetic mean of 3.32, higher than the hypothetical mean (3). However, the standard deviation shows that the opinions of the research sample were homogeneous, reaching 0.87 with a percentage of 70.4%, indicating that the sample's trend was towards (agree), indicating that the research sample agreed with the paragraphs of the second axis. Table No. (8) provides the analytical description of the axis paragraphs as follows:

Table (8) shows the statistical results (arithmetic mean, standard deviation and percentages)

Paragraphs	arithmetic mean	standard deviation	percentage	Sample orientation
1	3.54	0.8	70.8	I agree
2	3.32	0.87	66.4	neutral
3	3.49	0.86	69.8	I agree
For the fifth dimension as a whole	**3.32**	**0.87**	**70.4**	**I agree**

The table was prepared by the researcher using SPSS 1.0.

4.5.1. An examination of the opening paragraph: The sample views paragraph No. (1), which states that "the application of blockchains leads to raising the level of trust and security in all digital banking services," as "agreeing," as indicated by its arithmetic mean of 3.54, which is higher than 3.40 and lower than 4.19. In order to determine how far the responses of the participants in paragraph (1) deviate from the arithmetic mean, it is observed that the standard deviation is 0.8, indicating that the responses are less scattered and more uniform, and the percentage is 70.8%, indicating that the sample has a tendency to agree.

4.5.2. Interpretation of the second paragraph: With an arithmetic mean of (3.32), which is higher than (2.60) and lower than (3.39), paragraph No. (2), which reads, "I see that the characteristics of blockchains combined (stability, decentralization...etc.) provide a structural solution to reduce current security risks," illustrates the sample's (neutral) opinion of the statement. The standard deviation of the responses to paragraph (2) is 0.87, indicating that they are less dispersed and more homogeneous, and the percentage is 66.4%, indicating that the sample has a tendency towards neutrality. These findings indicate the degree of deviation of the responses from the arithmetic mean.

4.5.3. Interpretation of the third paragraph: An arithmetic mean of 3.49, which is higher than 3.40 and lower than 4.19, indicates that the sample believes that paragraph No. (3), which claims that "the security of digital financial data in the bank will be more reliable after adopting blockchain technology," is true. In order to determine the degree of departure of the responses of the individuals to paragraph (3) from the arithmetic mean, it is observed that the standard deviation is (0.86), indicating that the responses are less distributed and more uniform, and the percentage is (69.8%), indicating that the sample has a tendency to agree.

5.Testing hypotheses of influence between variables

Main hypothesis: There is a significant impact of the effectiveness of blockchain technology in protecting digital financial data.

Given that block chain technology involves four independent variables denoted by (x_4, x_3, x_2, x_1), a suitable hypothesis must be developed in order to investigate its effects. In order to investigate the hypothesis, a suitable model for the data that appropriately captures the research problem must be created. The dependent variable, security of digital financial data, is represented by the protection of digital financial data According to Table 9, once the impact has been measured and the best model for the data has been selected, the coefficient of determination (the coefficient of determination of the best model) is 0.818 = R^2, which indicates that the independent variables account for 81% of the effect on the dependent variable (y). The remaining 9% is either attributed to unknown errors or is thought to be random errors in selecting the particular answer. R=0.904, the value obtained when assessing the role of the relationship between the variables, shows that the relationship is strong. Regarding the test value (F=22.902), which examines the appropriateness of the data regression line By rejecting the null hypothesis and accepting the alternative hypothesis—that is, the existence of an impact of blockchain technology that results in the protection of digital financial data—the regression model's null hypothesis, which was (0.000), which is less than (0.05), indicated that there were no significant differences and that the model accurately represented the phenomenon under study. The regression line also fit the data. After passing the t test, the coefficient (β), which shows how each independent variable affects data security at a significance level below 0.05, is presented. In other words, there is a direct and substantial relationship.

Table No. (9) shows the coefficient of determination of the best model and the amount of influence of the independent variables.

Model Summary						
Model		R	R Square[b]	Adjusted R Square		F
1		.904[a]	.818	.782		22.902
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	x1	.243	.155	.262	1.564	.024
	x2	.298	.173	.326	1.719	.002
	x3	.239	.147	.254	1.633	.009
	x4	.140	.167	.146	.837	.007
a. Dependent Variable: y						
b. Regression Linearity via the Origin						

Chapter Four: Results and recommendations

1. Results

- A direct, statistically significant, and meaningful positive impact of blockchain technology on the protection of digital financial data has been demonstrated.
- The independent variables (block chain characteristics) account for 81% of the variance in the dependent variable (digital financial data security), confirming that the model accurately represents the phenomenon under study.
- Block chain technology is a fundamental solution to address security challenges in the banking sector, thanks to its basic characteristics such as immutability, as the inability to modify or delete prevents fraud and manipulation of transactions and financial records after they have been added.
- The decentralization feature helps to improve the security of digital financial data because it makes it impossible to fully compromise the system at once by distributing records among many participants, or nodes.

• Traditional methods of safeguarding financial data are no longer effective against modern cyber threats, so the development of data security systems is essential. When compared to traditional high-speed payment systems, scalability is one of the biggest barriers to banks' adoption of technology since growing network operations may lead to slower and more expensive processes.

2. Recommendations

1. Iraqi commercial banks must begin developing strategic plans to integrate block chain technology with their current security framework in order to increase the security and reliability of their digital financial data.
2. The banking sector's transition to a secure digital transformation should be streamlined, with a focus on decentralized verification and knowledge of encryption techniques.
3. In order to overcome the scalability problem that could hinder the integration of technology in large banking operations, banks and regulators should focus on selecting proprietary block chain systems or looking into Layer 2 solutions that have the capacity to process transactions efficiently and rapidly.
4. For the banking industry to use block chain technology safely and effectively, decision-makers and regulators (like the central bank and the Securities and Exchange Commission) must create clear laws and policies. This will increase user trust and lower regulatory risks.
5. It is necessary to work on updating old banking systems to ensure their ability to effectively support block chain technology and facilitate its integration, in order to reduce the complexity resulting from combining decentralized technology with centralized mechanisms.
6. Investing in training and raising awareness among banking sector employees about the mechanisms and principles of block chain technology.

References

1. Abdel Halim, A. H. M., Omran, R. M., & Al-Khatib, M. M. A. L. (2025). The Impact of Using Blockchain Technology on Improving the Quality of Disclosure of Future Information. Journal of Accounting Innovation, 2(4).
2. Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. World Journal of Advanced Research and Reviews, 20(3), 1743–1756.
3. Ali, S. I. (2021). Blockchain Technology as a Mechanism for Governing Contemporary Islamic Financial Institutions. AQU Journal of Islamic Economics, 1(1).
4. Bank for International Settlements (BIS). (2023). FinTech and the Digital Transformation of Financial Services: Challenges and Opportunities for the Global Financial System. BIS.
5. Cho Man, & Park Soojin. (2021). Financial Consumer Protection in the Era of Digital Transformation: A critical survey of literature and policy practices (Vol. 01). the KDI School sponsored research project.
6. El-Naqeeb, A. M., & Abdel-Azim, M. H. (2024). The Role of Blockchain Technology in Improving the Training Process with Application to Employees of the National Bank of Egypt. Journal of Administrative Research, 3(42).
7. Financial Stability Board (FSB). (2024). Cyber Resilience in the Financial Sector: Progress and the Way Ahead. FSB.
8. Gyimah, K. N., Asiedu, E., & Antwi, F. (2023). Adoption of blockchain technology in the banking sector of Ghana: Opportunities and challenges. African Journal of Business Management, 17(2), 32–42
9. Hamad Moussa Ali Shehata, Emad Ali Mustafa Selim, & Israa Saadi Mohamed Zeidan. (2024). Measuring the Impact of Using Blockchain Technology on the Quality of Financial Reports: Applied Evidence in Egyptian Commercial Banks. Journal of Accounting Innovation, 2.
10. International Accounting Standards Board (IASB). (2018). Conceptual Framework for Financial Reporting. IFRS Foundation.
11. Jimmy, F. (2024). Enhancing data security in financial institutions with blockchain technology. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 5(1), 424–437.
12. Kentache, S., & Hachman, M. (2025). Smart contracts integrated into the digital blockchain: a tool to stimulate foreign trade and improve the performance of the banking system. Journal of Economic Geography, (02).
13. Mafike, R., & Mawela, T. (2022). Integrating blockchain into traditional financial systems: Challenges and solutions. African Journal of Information Systems, 14(1), 10–25.
14. Mafike, S. S., & Mawela, T. (2022). Blockchain design and implementation techniques, considerations and challenges in the banking sector: a systematic literature review.

15. Martino, P. (2019). Blockchain technology: Challenges and opportunities for banks. International Journal of Financial Innovation in Banking, 2(4), 314–333.
16. Mishra, L., & Kaushik, V. (2023). Application of blockchain in dealing with sustainability issues and challenges of financial sector. Journal of Sustainable Finance & Investment, 13(3), 1318–1333.
17. Muhammad, S. K. A. (2025). The impact of applying blockchain technologies on the effectiveness of the internal control system: A case study on the National Bank of Egypt. Journal of Accounting Innovation, 2(2).
18. Naimi-Sadigh, A., Asgari, T., & Rabiei, M. (2022). Digital transformation in the value chain disruption of banking services. Journal of the Knowledge Economy, 13(2), 1212–1242.
19. Omolara, P. O., Temitayo, O. A., & Paschal, M. E. (2024). Encryption techniques for financial data security in fintech applications. International Journal of Science and Research Archive, 12(01).
20. Ramyar Razkar Ahmad. (2021). The Role of Electronic Accounting Information Systems in Enhancing the Security of Financial Information. International Journal of Humanities and Social Sciences, 24.
21. Rania Sultan Mohammed Abdulhameed. (2021). The Impact of Blockchain Technology on the Accounting Environment in Egypt. College of Business Administration/Taif University.
22. Vaigandla, K. K., Karne, R., Siluveru, M., & Kesoju, M. (2023). Review on blockchain technology: architecture, characteristics, benefits, algorithms, challenges and applications. Mesopotamian journal of Cybersecurity, 2023, 73–84.
23. Vaigandla, S., Pavan, S. S., & Madhu, K. M. (2023). Blockchain in finance and supply chain: Current trends, challenges and future research directions. International Journal of Engineering Business Management, 15(1), 1–13.
24. Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. International Journal of Information Management, 52, 102090.
25. Wasel, A. A. H. M., & Aliwa, N. I. M. (2025, March). The Impact of Blockchain Technology as a Mechanism for Digital Transformation on the Financial Performance of Commercial Banks Operating in Egypt: An Applied Study. Journal of Financial, Administrative and Quantitative Research, Faculty of Commerce - Suez University, 1(5).
26. Zwaid, J. G., Mhawesh, A. H., & Hussein, A. H. (2020). Confidentiality, integrity and availability of accounting information reflected in enhancing the quality of financial inspections by using hotels as a case study. African Journal of Hospitality, Tourism and Leisure, 9(2).